DERBYSHIRE DALES DISTRICT COUNCIL

This information is available free of charge in electronic, audio, Braille and large print versions on request.

For assistance in understanding or reading this document or specific information about this Agenda or on the "Public Participation" initiative please call Democratic Services on 01629 761133 or e-mail committee@derbyshiredales.gov.uk

6 September 2017

To: All Councillors

As a Member or Substitute of the **Governance and Resources Committee**, please treat this as your summons to attend a meeting on **Thursday 14 September 2017 at 6.00pm in the Council Chamber, Town Hall, Matlock.**

Yours sincerely

Sandra Lamb
Head of Corporate Services

AGENDA

1. APOLOGIES/SUBSTITUTES

Please advise Democratic Services on 01629 761133 or e-mail committee@derbyshiredales.gov.uk of any apologies for absence and substitute arrangements.

2. APPROVAL OF MINUTES OF PREVIOUS MEETING

29 June 2017

3. PUBLIC PARTICIPATION

To enable members of the public to ask questions, express views or present petitions, **IF NOTICE HAS BEEN GIVEN**, (by telephone, in writing or by electronic mail) **BY NO LATER THAN 12 NOON OF THE WORKING DAY PRECEDING THE MEETING**.

4. INTERESTS

Members are required to declare the existence and nature of any interests they may have in subsequent agenda items in accordance with the District Council's Code of Conduct. Those interests are matters that relate to money or that which can be valued in money, affecting the Member her/his partner, extended family and close friends.

Published 6 September 2017

Interests that become apparent at a later stage in the proceedings may be declared at that time.

5. QUESTIONS PURSUANT TO RULE OF PROCEDURE NUMBER 15.

To answer questions from Members who have given the appropriate notice.

Page No.

6. EXTERNAL AUDITOR'S REPORT FOR 2016/17 ACCOUNTS **4 - 33**

To receive the External Auditor's report for 2016/17.

7. STATEMENT OF ACCOUNTS 2016/17 **34 - 39**

To consider approval of the Statement of Accounts for 2016/17.

NB: APPENDIX 2 - DRAFT STATEMENT OF ACCOUNTS 2016/17 – PUBLISHED SEPARATELY

8. LETTER OF REPRESENTATION 2016/17 **40 - 48**

To consider and approve the draft Letter of Representation as part of Members responsibility for approving the financial statements.

9. COMMUNICATIONS AND MARKETING STRATEGY **49 - 70**

To note the strategic framework of the current Communications and Marketing strategy and consider approval of the action plan for 2017/2018. Also to consider approval for a supplementary revenue estimate of £5,000 to enable the signage works to be completed in 2017/18.

10. CCTV DATA PROTECTION AND COMPLIANCE **71 - 72**

To consider a recommendation that expenditure of £11,100 from the General Reserve be approved to enable an increase in working hours for the current CCTV Manager.

11. INFORMATION SECURITY POLICY **73 - 134**

To consider approval of the 2017 revision of the Information Security Policy.

12. ICT PROJECTS FOR CAPITAL PROGRAMME 2017-19 **135 - 137**

To consider approval for additional capital projects related to ICT in 2017/18 and 2018/19.

13. LAND HOLDINGS REVIEW **138 - 146**

To consider 2 sites across the District in which expressions of interest or requests to purchase a site or granting a lease have been received and the terms which would apply.

14. COMPLAINTS MONITORING **147 - 161**

To receive information on formal complaints made under the Council's internal Complaints Procedures; those referred to the Local Government Ombudsman and those against individual elected member behaviour at town, parish and District Council level. Also to consider the recommendation to amend the Complaints Procedure as detailed in the report.

15. POLICY FOR COUNCIL TAX DISCRETIONARY RELIEF UNDER SECTION 13A (1)(c) OF THE LOCAL GOVERNMENT FINANCE ACT 1992 **162 - 169**

To consider approval of the adoption of a policy and the granting of delegated authority relating to Council Tax Discretionary Relief.

16. APPOINTMENT OF EXTERNAL AUDITOR **170 – 174**

To consider the recommendation by Public Sector Audit Appointments Limited that Mazars LLP be appointed as the Council's External Auditors from 2018/19 for the next five years.

Members of the Committee - Councillors Deborah Botham, Albert Catt, Steve Flitter, Chris Furness (Vice Chair), Alyson Hill, Neil Horton, Angus Jenkins, Tony Millward BEM, Jean Monks, Garry Purdy, Mike Ratcliffe, Lewis Rose, Mark Salt, Jacquie Stevens (Chairman), Colin Swindell, John Tibenham, Jo Wild

Substitutes – Councillors Jason Atkin, Richard Bright, Jennifer Bower, Sue Bull, Sue Burfoot, David Chapman, Tom Donnelly, Ann Elliott, Helen Froggatt, Susan Hobson, Richard FitzHerbert, Vicky Massey-Bloodworth, Joyce Pawley, Irene Ratcliffe, Philippa Tilbrook

Published 6 September 2017

NOT CONFIDENTIAL – For public release Item No. 6

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Resources

EXTERNAL AUDITOR'S REPORT FOR 2016/17 ACCOUNTS

PURPOSE OF REPORT

This report summarises the key findings arising from:

- The external auditor's work in relation to the Authority's 2016/17 financial statements; and
- The work to support the external auditor's 2016/17 conclusion on the Authority's arrangements to secure economy, efficiency and effectiveness in its use of resources ('VFM conclusion').

RECOMMENDATION

That the "External Auditor's Report 2016/17" is noted.

WARDS AFFECTED

None

STRATEGIC LINK

None

---

1 REPORT

1.1 The Council's external auditors, KPMG, have issued their report on the 2016/17 accounts and Value for Money (VFM) conclusion. A copy of the report is shown at Appendix 1. The external auditor has requested that it be brought to Members' attention.

1.2 The key issues in the report relating to the final accounts are:

- Subject to all outstanding queries being resolved to the auditors' satisfaction they anticipate issuing an unqualified audit opinion on the Authority's financial statements before the deadline of 30 September;
- The report identifies a significant audit risk relating to significant changes in the pension liability due to LGPS Triennial Valuation
- The report has three recommendations relating to the 2016/17 accounts. These are shown in Appendix 1 to the Auditor's report, together with the management response. The recommendations relate to:
    1. Management review of pension assumptions;
    2. The alignment of the Members' outturn report to the Narrative Statement contained in the Statement of Accounts;
    3. Availability of working papers.

1.3 The external auditor anticipates issuing an unqualified value for money conclusion.

2 RISK ASSESSMENT

2.1 Legal

There are no legal risks arising from this report.

2.2 Financial

There are no financial risks arising from this report.

3 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

4 CONTACT INFORMATION

Karen Henriksen, Head of Resources, Telephone: 01629 761284
e-mail: karen.henriksen@derbyshiredales.gov.uk

5 ATTACHMENTS

Appendix 1 – External Audit Report 2016/17

KPMG

External audit report 2016/17

Derbyshire Dales District Council

—

11 September 2017

Summary for Governance and Resources Committee

Financial statements

This document summarises the key findings in relation to our 2016-17 external audit at Derbyshire Dales District Council ('the Authority').

This report focusses on our on-site work which was completed in June 2017 on the Authority's significant risk areas, as well as other areas of your financial statements. Our findings are summarised on pages 4 – 5.

Our report also includes additional findings in respect of our control work which we have identified as part of our interim audit.

Subject to all outstanding queries being resolved to our satisfaction we anticipate issuing an unqualified audit opinion on the Authority's financial statements before the deadline of 30 September.

Our audit of the Authority's financial statements has not identified any audit adjustments which impact on the bottom line figures reported in the core statements. We have, however, identified a number of minor presentational issues. We understand that the Authority has amended the statements for all such issues identified. Further details can be seen in Appendix one.

Based on our work, we have raised 2 recommendations. Details on our recommendations can be found in Appendix 1.

Our audit is substantially complete however matters communicated in this Report may change pending receipt of further evidence on the below items. We will provide a verbal update on the status of our audit at the Governance and Resources Committee meeting but would highlight the following work is still outstanding:

- Reconciliation of the member's outturn report to the CIES;
- Receipt of final accounts;
- Final review of amended accounts; and
- Letter of Management Representation.

We anticipate issuing our completion certificate and Annual Audit letter by the deadline of 30 September.

Use of resources

We have completed our risk-based work to consider whether in all significant respects the Authority has proper arrangements to ensure has taken properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people. We have concluded that the Authority has made proper arrangements to secure economy, efficiency and effectiveness in its use of resources.

We therefore anticipate issuing an unqualified value for money opinion.

See further details on page 14.

Acknowledgements

We would like to take this opportunity to thank officers and Members for their continuing help and co-operation throughout our audit work.

We ask the Governance and Resources Committee to note this report.

Contents

The key contacts in relation to our audit are:

John Cornett
Director
KPMG LLP (UK)

+44 (0)785 447 9705
John.Cornett@kpmg.co.uk

Katie Scott
Assistant Manager
KPMG LLP (UK)

+44 (0)746 836 5923
Katie.Scott@kpmg.co.uk

Arvinder Khela
Audit In-charge
KPMG LLP (UK)

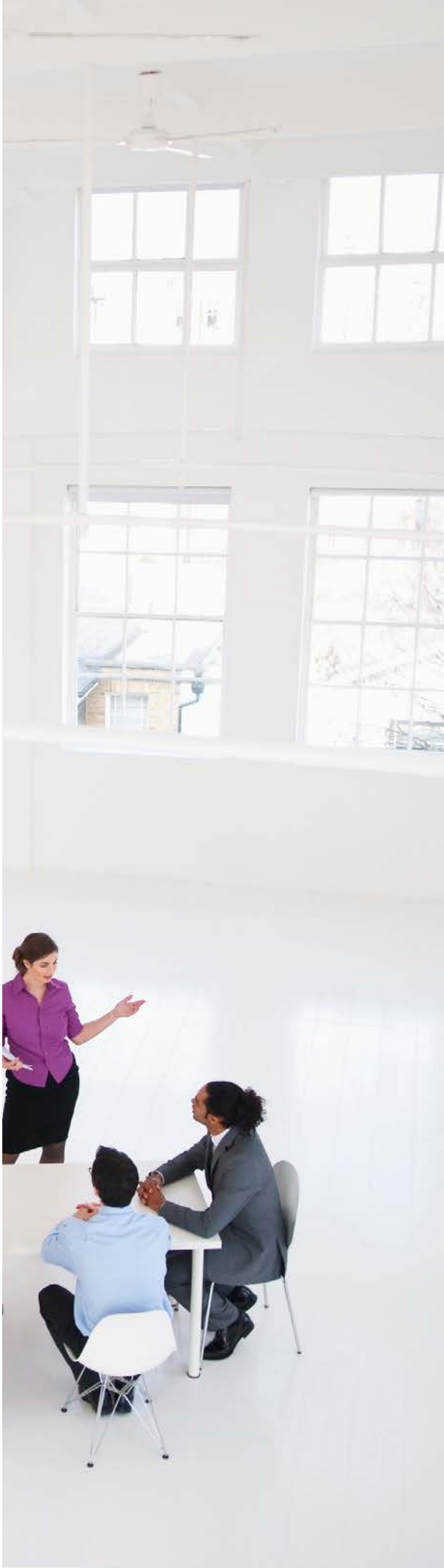
+44 (0)750 099 0073
Arvinder.Khela@kpmg.co.uk

Section one

Financial Statements

We anticipate issuing an unqualified audit opinion on the Authority's 2016/17 financial statements by 30 September 2017. We will also report that your Annual Governance Statement complies with the guidance issued by CIPFA/SOLACE (*'Delivering Good Governance in Local Government'*) published in April 2016.

For the year ending 31 March 2017, the Authority has reported under the provision of services total income of £38.7 million against expenditure of £39.4 million. This has resulted in a net funding requirement on the provision of services of £0.6 million. The impact has been a decrease in the General Fund.



Significant audit risks

Our *External Audit Plan 2016/17* sets out our assessment of the Authority's significant audit risks. We have completed our testing in these areas and set out our evaluation following our work:

Significant audit risks	Work performed
1. Significant changes in the pension liability due to LGPS Triennial Valuation	**Why is this a risk?** During the year, the Pension Fund has undergone a triennial valuation with an effective date of 31 March 2016 in line with the *Local Government Pension Scheme (Administration) Regulations 2013*. The share of pensions assets and liabilities for each admitted body is determined in detail, and a large volume of data is provided to the actuary to support this triennial valuation. There is a risk that the data provided to the actuary for the valuation exercise is inaccurate and that these inaccuracies affect the actuarial figures in the accounts. Most of the data is provided to the actuary by Derbyshire County Council who administer the Pension Fund. **Our work to address this risk** We have reviewed the process used to submit payroll data to the Pension Fund and have found no issues to note. We have also tested the year-end submission process and agreed pension costs, liabilities and disclosures under IAS19 to confirmations from the scheme actuary. We found that there was no management review of actuarial assumptions. Management has subsequently confirmed that the assumptions used by the actuary are appropriate. Nonetheless, there is a risk that the inappropriate assumptions were used by the actuary to calculate the Authority's pension liability, thus potentially resulting in an incorrect liability being recognised. We have raised a recommendation that actuarial assumptions should be reviewed to ensure that they are appropriate for the Authority, see recommendation 1. We have liaised with our own internal actuary as well as engaged with your Pension Fund audit team to gain assurance over the pensions figures. Testing carried out at the Pension Fund We liaised with your Pension Fund audit team to gain assurance over: — the operation of the Fund's controls, including the controls over the transfer of data to the actuary; — the figures submitted from the Fund to the actuary, including the completeness and accuracy of the data; — investment balances;

Considerations required by professional standards

Fraud risk of revenue recognition

Professional standards require us to make a rebuttable presumption that the fraud risk from revenue recognition is a significant risk.

In our *External Audit Plan 2016/17* we reported that we do not consider this to be a significant risk for Local Authorities as there is unlikely to be an incentive to fraudulently recognise revenue.

This is still the case. Since we have rebutted this presumed risk, there has been no impact on our audit work.

Management override of controls

Professional standards require us to communicate the fraud risk from management override of controls as significant because management is typically in a unique position to perpetrate fraud because of its ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively.

Our audit methodology incorporates the risk of management override as a default significant risk. We have not identified any specific additional risks of management override relating to this audit.

In line with our methodology, we carried out appropriate controls testing and substantive procedures, including over journal entries, accounting estimates and significant transactions that are outside the normal course of business, or are otherwise unusual.

There are no matters arising from this work that we need to bring to your attention.

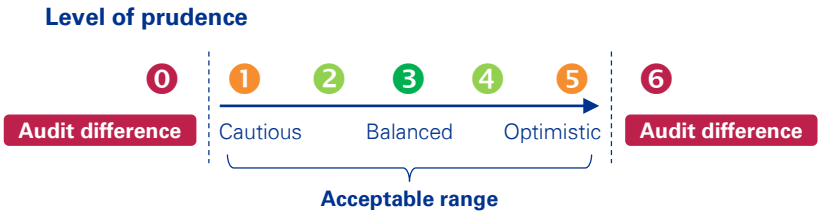
Other areas of audit focus

We identified one area of audit focus. This is not considered as a significant risk as it is less likely to give rise to a material error. Nonetheless this is a area of importance where we would carry out substantive audit procedures to ensure that there is no risk of material misstatement.

Other areas of audit focus	Our work to address the areas
1. Disclosures associated with retrospective restatement of CIES, EFA and MiRS	**Background** CIPFA has introduced changes to the 2016/17 Local Government Accounting Code (Code): — Allowing local authorities to report on the same basis as they are organised by removing the requirement for the Service Reporting Code of Practice (SeRCOP) to be applied to the Comprehensive Income and Expenditure Statement (CIES); and — Introducing an Expenditure and Funding Analysis (EFA) which provides a direct reconciliation between the way local authorities are funded and prepare their budget and the CIES. This analysis is supported by a streamlined Movement in Reserves Statement (MiRS) and replaces the current segmental reporting note. The Authority was required to make a retrospective restatement of its CIES (cost of services) and the MiRS. New disclosure requirements and restatement of accounts require compliance with relevant guidance and correct application of applicable accounting standards. **What we have done** For the restatement, we have obtained an understanding of the methodology used to prepare the revised statements. We have also agreed figures disclosed to the Authority's general ledger. However we have raised a recommendation that the outturn report that is reported to members is aligned with how the outturn is reported to budget holders, see recommendation 2.

Judgements

We have considered the level of prudence within key judgements in your 2016/17 financial statements and accounting estimates. We have set out our view below across the following range of judgements.



Subjective areas	2016/17	2015/16	Commentary
Provisions (including NDR)	4	4	Short term provisions amounted to £254k and long term provisions £50k for 2016/17 . There has been no material movement from the prior year which is in line with our expectations. The main proportion of the provision was in relation to NNDR appeals and the movement in year has not been material. We consider the provision disclosures to be proportionate.
PPE: valuation of assets and asset lives	3	3	The Authority has utilised an internal valuation expert to provide valuation estimates. We have reviewed the instructions provided and deem that the valuation exercise is in line with the instructions. The resulting increase of is in line with regional indices provided by Gerald Eve, the valuation firm engaged by the NAO to provide supporting valuation information.

Proposed opinion and audit differences

Subject to all outstanding queries being resolved to our satisfaction, we anticipate issuing an unqualified audit opinion on the Authority's 2016/17 financial statements following approval of the Statement of Accounts by the Governance and Resources Committee on 14 September 2017.

Status of our audit

Our audit is substantially complete however matters communicated in this Report may change pending receipt of further evidence on the below items. We will provide a verbal update on the status of our audit at the Governance and Resources Committee meeting but would highlight the following work is still outstanding:

- Reconciliation of the member's outturn report to the CIES;
- Receipt of final accounts;
- Final review of amended accounts; and
- Letter of Management Representation.

Audit differences

In accordance with ISA 260 we are required to report uncorrected audit differences to you. We also report any material misstatements which have been corrected and which we believe should be communicated to you to help you meet your governance responsibilities.

The final materiality (see Appendix 4 for more information on materiality) level for this year's audit was set at £700k. Audit differences below £35k are not considered significant.

We did not identify any material misstatements. We identified a number of issues that have been adjusted by management however these mainly were presentational and thus did not have a material effect on the financial statements.

Annual governance statement

We have reviewed the Authority's 2016/17 Annual Governance Statement and confirmed that:

— It complies with *Delivering Good Governance in Local Government: A Framework published by CIPFA/SOLACE*;

— It is not misleading or inconsistent with other information we are aware of from our audit of the financial statements.

Narrative report

We have reviewed the Authority's 2016/17 narrative report and have confirmed that it is consistent with the financial statements and our understanding of the Authority.

Accounts production and audit process

Our audit standards (*ISA 260*) require us to communicate our views on the significant qualitative aspects of the Authority's accounting practices and financial reporting.

We also assessed the Authority's process for preparing the accounts and its support for an efficient audit. The efficient production of the financial statements and good-quality working papers are critical to meeting the tighter deadlines.

Accounting practices and financial reporting

The Authority has recognised the additional pressures which the earlier closedown in 2017/18 will bring. We have been engaging with the Authority in the period leading up to the year end in order to proactively address issues as they emerge.

We experienced delays in obtaining evidence to support our testing, for example in relation to PPE valuations and the CIES restatement, from the Authority. The delays have meant that we spent additional time over and above what was originally planned.

We consider the Authority's accounting practices appropriate.

Completeness of draft accounts

We received a complete set of accounts for audit on 26 May 2017, which was a month in advance of the statutory deadline.

Quality of supporting working papers

We issued our *Accounts Audit Protocol 2016/17* ("Prepared by Client" request) in April 2017 which outlined our documentation request. This helps the Authority to provide audit evidence in line with our expectations.

The Authority's finance team has produced good quality working papers that were referenced to the "Prepared by client" schedule. The departure of a key member of staff prior to the audit process did cause some difficulties for the finance team and we have raised a recommendation around the backing to non-material notes in the accounts.

Response to audit queries

Officers dealt with our audit queries efficiently, responding within appropriate timescales. As a result of this, we were able to complete most of our on-site work within the agreed timescales. However, the delays (referred to above) in some areas of testing left a proportion of our work that needed to be completed after the team had finished on-site and had moved onto other audits.

Prior year recommendations

As part of our audit we have specifically followed up the Authority's progress in addressing the recommendations in last years ISA 260 report.

The Authority has implemented all of the recommendations in our ISA 260 Report 2015/16.

Appendix 2 provides further details.

Controls over key financial systems

We have tested controls as part of our focus on significant audit risks and other parts of your key financial systems on which we rely as part of our audit. The strength of the control framework informs the substantive testing we complete during our final accounts visit.

Below we have highlighted exceptions, identified through our work, in relation to controls:

Journals

— Authorisation of journals is done through a report of individual journal lines over £30k rather than the absolute debit/credit balance over £30k.

Pensions

— Management review of approval of actuarial assumptions does not occur. Instead reliance is placed on Pension Fund administrators to review the actuarial assumptions. We have places reliance on the assurance from the Pension Fund auditor and our actuary specialists.

Further detail and associated recommendations can be found in Appendix 1.

Completion

We confirm that we have complied with requirements on objectivity and independence in relation to this year's audit of the Authority's 2016/17 financial statements.

Before we can issue our opinion we require a signed management representation letter.

Once we have finalised our opinions and conclusions we will prepare our Annual Audit Letter and close our audit.

Declaration of independence and objectivity

As part of the finalisation process we are required to provide you with representations concerning our independence.

In relation to the audit of the financial statements of Derbyshire Dales District Council for the year ending 31 March 2017, we confirm that there were no relationships between KPMG LLP and Derbyshire Dales District Council, its directors and senior management and its affiliates that we consider may reasonably be thought to bear on the objectivity and independence of the audit engagement lead and audit staff. We also confirm that we have complied with Ethical Standards and the Public Sector Audit Appointments Ltd requirements in relation to independence and objectivity.

We have provided a detailed declaration in Appendix 5 in accordance with ISA 260.

Management representations

You are required to provide us with representations on specific matters such as your financial standing and whether the transactions within the accounts are legal and unaffected by fraud. We have provided a template to Karen Henriksen – Head of Resources for presentation to the Governance and Resources Committee. We require a signed copy of your management representations before we issue our audit opinion.

Other matters

ISA 260 requires us to communicate to you by exception 'audit matters of governance interest that arise from the audit of the financial statements' which include:

- Significant difficulties encountered during the audit;
- Significant matters arising from the audit that were discussed, or subject to correspondence with management;
- Other matters, if arising from the audit that, in the auditor's professional judgment, are significant to the oversight of the financial reporting process; and
- Matters specifically required by other auditing standards to be communicated to those charged with governance (e.g. significant deficiencies in internal control; issues relating to fraud, compliance with laws and regulations, subsequent events, non disclosure, related party, public interest reporting, questions/objections, opening balances etc.).

There are no others matters which we wish to draw to your attention in addition to those highlighted in this report or our previous reports relating to the audit of the Authority's 2015/16 financial statements.

Section two

Value for money

Our 2016/17 VFM conclusion considers whether the Authority had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.

We have concluded that the Authority has made proper arrangements to ensure it took properly-informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.

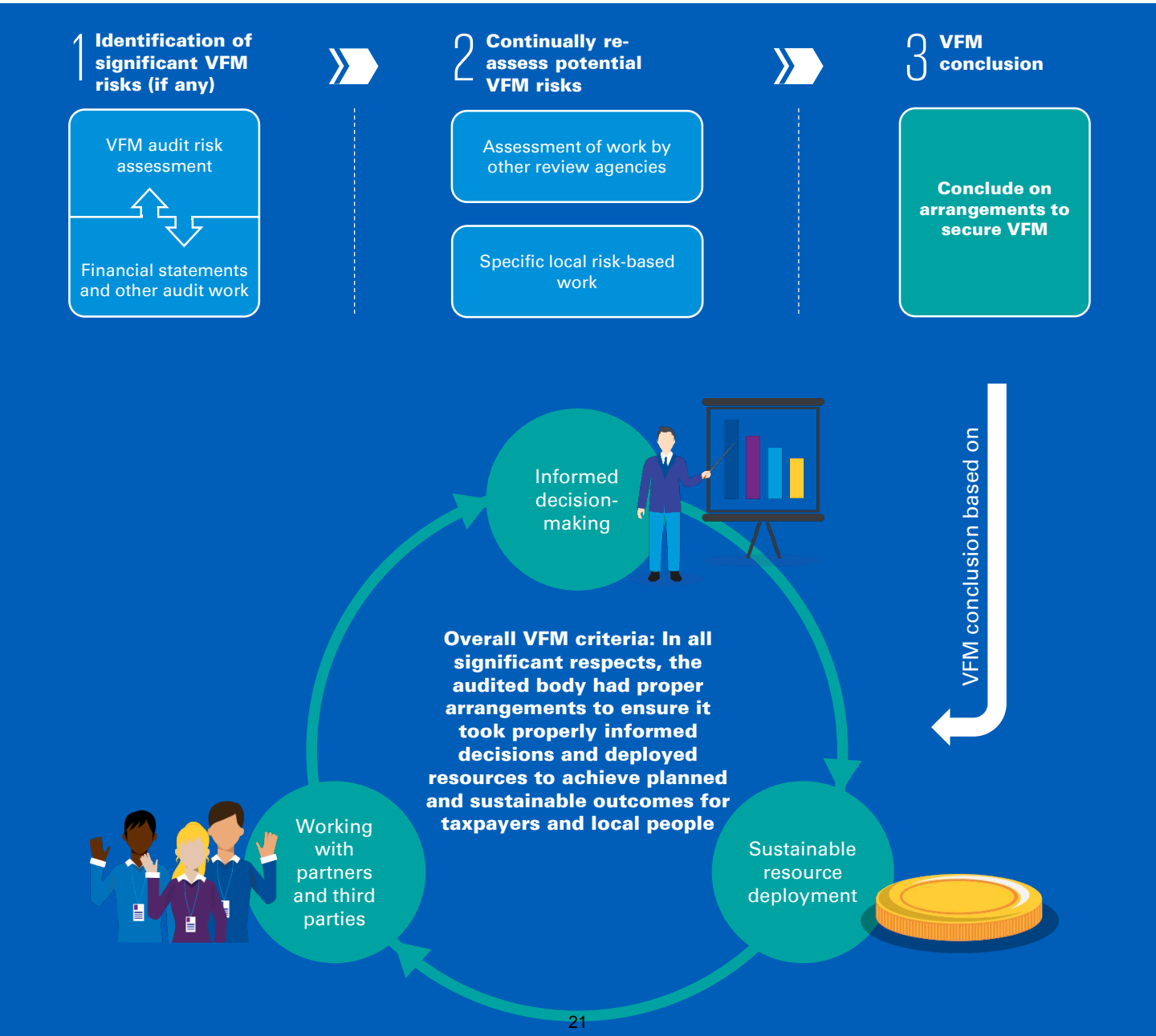
VFM conclusion

The Local Audit and Accountability Act 2014 requires auditors of local government bodies to be satisfied that the authority 'has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources'.

This is supported by the Code of Audit Practice, published by the NAO in April 2015, which requires auditors to 'take into account their knowledge of the relevant local sector as a whole, and the audited body specifically, to identify any risks that, in the auditor's judgement, have the potential to cause the auditor to reach an inappropriate conclusion on the audited body's arrangements.'

Our VFM conclusion considers whether the Authority had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.

We follow a risk based approach to target audit effort on the areas of greatest audit risk.



We have identified one significant VFM risks, as communicated to you in our *2016/17 External Audit Plan*. We are satisfied that external or internal scrutiny provides sufficient assurance that the Authority's current arrangements in relation to these risk areas are adequate.

The table below summarises our assessment of the individual VFM risk identified against the three sub-criteria. This directly feeds into the overall VFM criteria and our value for money opinion.

VFM assessment summary			
VFM risk	**Informed decision-making**	**Sustainable resource deployment**	**Working with partners and third parties**
1. Delivery of the medium term financial plan.	✓	✓	✓
Overall summary	✓	✓	✓

In consideration of the above, we have concluded that in 2016/17, the Authority has made proper arrangements to ensure it took properly-informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.

Further details on the work done and our assessment are provided on the following pages.

Significant VFM risks

Significant VFM risks	Work performed
1. Delivery of the medium term financial plan.	**Why is this a risk?** There has been a significant shift in the national outlook over the last 12 months, primarily driven by the outcome of the referendum on 23 June 2016 on the UK's membership of the European Union. Consequently GDP growth forecasts have been revised downwards, which potentially reduces the level of any growth in business rates income. Inflationary pressures, service pressures, and a reduction in the local government finance settlement will impact on the Authority's finances. In November 2016, the Authority updated their Medium Term Financial Strategy (MTFS) for 2017/18 –2021/22 (which incorporates its Efficiency Plan). Since 2014, the Authority has achieved savings of £0.9 million and is, therefore, well placed to meet the challenges going forward. The Authority does however recognise that this will be no easy task. From 2018/19, the Authority has identified funding gaps and is forecasting a corporate savings target of £0.5 million. The council recognises that this target is challenging and it equates to 5% of forecast spending in 2018/19. Savings of £1.2 million are required by 2021/22. This equates to 12% of net revenue spending using 2016/17 as a baseline position. Savings of this magnitude will require fundamental changes in the way the Council operates and Members may need to take increasingly difficult decisions going forward. However, Officers are confident that the Efficiency Plan contained within the MTFS sets out the Council's approach to meet the corporate savings target and closing the budget gap over the next five years. There are risks associated with this approach and these are explained in the MTFS. Key assumptions built into the strategy have specifically focussed on anticipated further reductions in government funding, the impact of the 2017 business rates revaluation and the proposed changes to the business rate retention scheme. **Summary of our work** Like most of local government, the Authority faces a challenging future driven by funding reductions and an increase in demand for services. At a local level, this is compounded by the County Council's financial difficulties. In reaching our VFM conclusion we have considered the Authority's arrangements for making properly informed decisions, sustainable resource deployment and working with partners and third parties. This has included detailed reviews of key documents including the Medium Term Financial Plan, Corporate Plan and Economic Plan. Our work also reflects the discussions we have held with key officers throughout the year regarding the Authority's continued plans for growth and income generation and cost savings. We have reviewed arrangements put in place by the Council to deliver savings through the annual budget process, the development of specific projects such as service reviews and a major exercise to identify savings across all services. The latest MTFP, revised June 2017, indicates a Corporate Savings target of £1.5 million will be achieved by 2021/22. This is an increase of £0.3 million from the November 2016 MTFP described above and uses the estimated 2017/18 figures rather than forecast to give a more realistic view.

Significant VFM risks	Work performed

(continued)

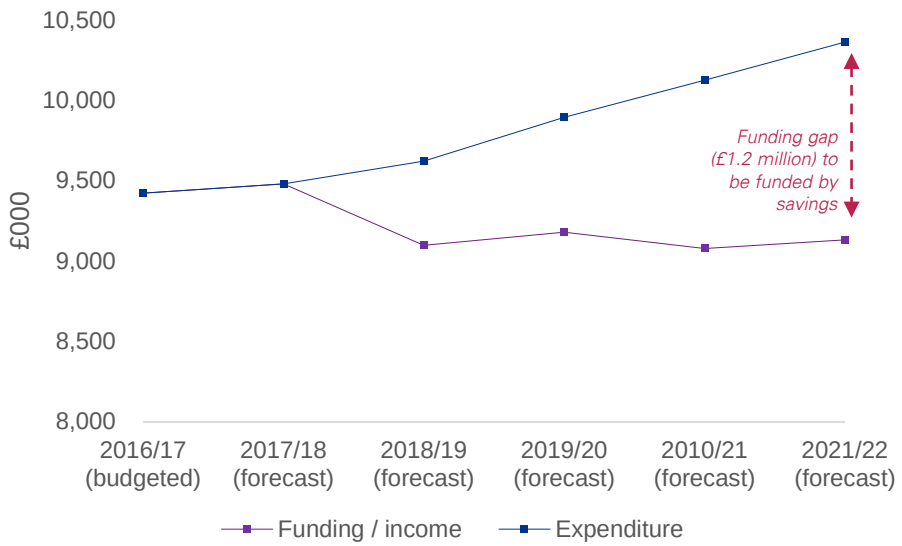
2016/17 Outturn

We reviewed the financial outturn position against original plans. The final outturn report that was taken to council on 22nd June 2017 showed that for 2016/17 there was an under-spend on the General Fund of £0.6 million when comparing the final expenditure with the revised budget.

This outturn position provides the Authority with its planned level of financial resilience against risks including uncertainties relating to the reduction in Government grants and NNDR, alongside some flexibility to enable it to invest either to save or to generate returns.

Given the scale of the challenge that faces the Authority in future years and the current funding uncertainties, it is important that these savings are secured by underlying reductions in expenditure or increases in income in order to secure the projected financial savings of £0.5 million which are anticipated to be required in 2018/19.

Chart 1: MTFP summary from 2016/17 to 2021/22 (from November 2016 MTFP)



Appendices

Appendix 1

Key issues and recommendations

Our audit work on the Authority's 2016/17 financial statements have identified a small number of presentational issues. These have been discussed with management and the financial statements have been amended for all of them. The main adjustment was in relation to grants as disclosed

The Authority should closely monitor progress in addressing the risks, including the implementation of our recommendations. We will formally follow up these recommendations next year.

Each issue and recommendation have been given a priority rating, which is explained below.

Issues that are fundamental and material to your system of internal control. We believe that these issues might mean that you do not meet a system objective or reduce (mitigate) a risk.

Issues that have an important effect on internal controls but do not need immediate action. You may still meet a system objective in full or in part or reduce (mitigate) a risk adequately but the weakness remains in the system.

Issues that would, if corrected, improve internal control in general but are not vital to the overall system. These are generally issues of good practice that we feel would benefit if introduced.

The following is a summary of the issues and recommendations raised in the year 2016/17.

2016/17 recommendations summary

Priority	Number raised from our year-end audit	Total raised for 2016/17
High	2	**2**
Medium	1	**1**
Low	0	**0**
Total	**3**	**3**

Appendix 1

High priority

1. Review of Pensions Assumptions

— Management review of the approval of actuarial assumptions used to calculate the pensions liability does not occur.

— The Authority instead place reliance on the Pension Fund administrators to review the actuarial assumptions on their behalf.

— The risk surrounding this focuses on the balance of the Pension liability and its material impact on the Financial Statements.

Recommendation

The Authority should review the actuaries' assumptions and ensure they align to the Authority's understanding and comprehend to the calculation of the Pension liability.

Management Response

Accepted

A management review of actuarial assumptions will be undertaken for Accounts relating to 2017/18 and subsequent years

Owner

Head of Resources

Deadline

31 May 2018

High priority

2. Alignment of Members outturn report to the Narrative Statement.

During our testing of the restatement of the CIES and the new requirement of the EFA, we have identified that the Authority reports it's outturn position to Members in a different manner to budget holders.

This resulted in the outturn report to Members being unreconciled to the Financial Statements.

Recommendation

The format of the outturn report, reported to members and budget holders should agree to one another. Additionally, it should also reconcile back to the Narrative Statement and the EFA statement,

Management Response

Accepted

A reconciliation between the outturn report and the Narrative Statement and EFA Statement was prepared on 16th August 2017, in respect of the 2016/17 accounts.

The format of the outturn report and budget holders' reports will be reviewed for 2017/18 accounts to improve the process for future years.

Owner

Head of Resources

Deadline

31 March 2018

Medium priority

3. Working Papers

Although the Authority has worked hard to deliver work papers provided, there were still not readily available work papers behind each note of the accounts as we would expect. This caused delays to our audit work as, as a result of the departure of key finance staff, information behind some notes was difficult to provide.

Recommendation

We recommend a work paper for each note is prepared to allow a clear audit trial between the ledger and the note in the accounts.

Management Response

Accepted

A working paper will be prepared for each note in the accounts for 2017/18 and subsequent years.

The recent approval for an additional senior accountant for a two year fixed period has increased the resources available to carry out this work, reducing the risk of future delays to the audit process.

Owner

Head of Resources

Deadline

30 May 2018

Appendix 2

Follow-up of prior year recommendations

In the previous year, we raised two recommendations which we reported in our *External Audit Report 2015/16 (ISA 260)*. The Authority has implemented all of the recommendations. We re-iterate the importance of the outstanding recommendations and recommend that these are implemented by the Authority.

We have used the same rating system as explained in Appendix 1.

Each recommendation is assessed during our 2016/17 work, and we have obtained the recommendation's status to date. We have also obtained Management's assessment of each outstanding recommendation.

Below is a summary of the prior year's recommendations.

2015/16 recommendations status summary

Priority	Number raised	Number implemented / superseded	Number outstanding
High	1	1	**0**
Medium	0	0	**0**
Low	1	1	**0**
Total	**2**	**2**	**0**

High priority

1. Working Papers and use of the Prepared by Client List

Prior to our interim visit, KPMG issue a PBC to update the Finance team with what will be required at Interim. Not all of the documents were available for the interim visit and again at final where many working papers, mainly regarding PPE, were not provided until the end of the site visit.

Recommendation

We recommend going forward that the Finance team follow up the PBC more closely and provide all documents requested to ensure a more efficient year end audit.

Management original response

Recommendation agreed. The finance team will follow the Prepared by Client List more closely when preparing the accounts for 2016/17 and will provide all documents and working papers by the agreed dates.

Owner

Accountancy & Exchequer Manager

Original deadline

2016/17 final accounts production

KPMG's July 2017 assessment

Fully implemented

Working papers provided both at interim and final were cross referenced to the PBC at Interim and Final.

Low priority

2. Formalisation of Valuer Instructions

We found no formal instructions were sent to the in-house valuer and therefore there was no audit trail for what had been asked for and the timescales expected.

Recommendation

We recommend a formal e-mail is sent to the valuer to confirm what is expected from him and when it is expected.

Management original response

Recommendation agreed. The finance team will issue formal instructions to the valuer to confirm the information that is expected and the key dates for the accounts for 2016/17.

Owner

Accountancy & Exchequer Manager

Original deadline

2016/17 final accounts production

KPMG's July 2017 assessment

Fully implemented

Within our testing of controls within PPE, we have found that instructions have been sent to the valuer over revaluations and scope includes impairment.

Appendix 3

Materiality and reporting of audit differences

The assessment of what is material is a matter of professional judgment and includes consideration of three aspects: materiality by value, nature and context.

Material errors by value are those which are simply of significant numerical size to distort the reader's perception of the financial statements. Our assessment of the threshold for this depends upon the size of key figures in the financial statements, as well as other factors such as the level of public interest in the financial statements.

Errors which are material by nature may not be large in value, but may concern accounting disclosures of key importance and sensitivity, for example the salaries of senior staff.

Errors that are material by context are those that would alter key figures in the financial statements from one result to another – for example, errors that change successful performance against a target to failure.

We used the same planning materiality reported in our External Audit Plan 2016/17, presented to you in February 2017.

Materiality for the Authority's accounts was set at £700k which equates to around 1.9 percent of gross expenditure. We design our procedures to detect errors in specific accounts at a lower level of precision.

Reporting to the Governance and Resources Committee

Whilst our audit procedures are designed to identify misstatements which are material to our opinion on the financial statements as a whole, we nevertheless report to the Governance and Resources Committee any misstatements of lesser amounts to the extent that these are identified by our audit work.

Under *ISA 260*, we are obliged to report omissions or misstatements other than those which are 'clearly trivial' to those charged with governance. *ISA 260* defines 'clearly trivial' as matters that are clearly inconsequential, whether taken individually or in aggregate and whether judged by any quantitative or qualitative criteria.

ISA 450 requires us to request that uncorrected misstatements are corrected.

In the context of the Authority, we propose that an individual difference could normally be considered to be clearly trivial if it is less than £35k for the Authority.

Where management have corrected material misstatements identified during the course of the audit, we will consider whether those corrections should be communicated to the Governance and Resources Committee to assist it in fulfilling its governance responsibilities.

Appendix 4

Declaration of independence and objectivity

Auditors appointed by Public Sector Audit Appointments Ltd must comply with the Code of Audit Practice (the 'Code') which states that:

> *"The auditor should carry out their work with integrity, objectivity and independence, and in accordance with the ethical framework applicable to auditors, including the ethical standards for auditors set by the Financial Reporting Council, and any additional requirements set out by the auditor's recognised supervisory body, or any other body charged with oversight of the auditor's independence. The auditor should be, and should be seen to be, impartial and independent. Accordingly, the auditor should not carry out any other work for an audited body if that work would impair their independence in carrying out any of their statutory duties, or might reasonably be perceived as doing so."*

In considering issues of independence and objectivity we consider relevant professional, regulatory and legal requirements and guidance, including the provisions of the Code, the detailed provisions of the Statement of Independence included within the Public Sector Audit Appointments Ltd Terms of Appointment ('Public Sector Audit Appointments Ltd Guidance') and the requirements of APB Ethical Standard 1 Integrity, Objectivity and Independence ('Ethical Standards').

The Code states that, in carrying out their audit of the financial statements, auditors should comply with auditing standards currently in force, and as may be amended from time to time. Public Sector Audit Appointments Ltd guidance requires appointed auditors to follow the provisions of *ISA (UK&I) 260 'Communication of Audit Matters with Those Charged with Governance'* that are applicable to the audit of listed companies. This means that the appointed auditor must disclose in writing:

- Details of all relationships between the auditor and the client, its directors and senior management and its affiliates, including all services provided by the audit firm and its network to the client, its directors and senior management and its affiliates, that the auditor considers may reasonably be thought to bear on the auditor's objectivity and independence.
- The related safeguards that are in place.
- The total amount of fees that the auditor and the auditor's network firms have charged to the client and its affiliates for the provision of services during the reporting period, analysed into appropriate categories, for example, statutory audit services, further audit services, tax advisory services and other non-audit services. For each category, the amounts of any future services which have been contracted or where a written proposal has been submitted are separately disclosed. We do this in our Annual Audit Letter.

Appointed auditors are also required to confirm in writing that they have complied with Ethical Standards and that, in the auditor's professional judgement, the auditor is independent and the auditor's objectivity is not compromised, or otherwise declare that the auditor has concerns that the auditor's objectivity and independence may be compromised and explaining the actions which necessarily follow from this. These matters should be discussed with the Governance and Resources Committee.

Ethical Standards require us to communicate to those charged with governance in writing at least annually all significant facts and matters, including those related to the provision of non-audit services and the safeguards put in place that, in our professional judgement, may reasonably be thought to bear on our independence and the objectivity of the Engagement Lead and the audit team.

General procedures to safeguard independence and objectivity

KPMG LLP is committed to being and being seen to be independent. As part of our ethics and independence policies, all KPMG LLP Audit Partners and staff annually confirm their compliance with our Ethics and Independence Manual including in particular that they have no prohibited shareholdings.

Our Ethics and Independence Manual is fully consistent with the requirements of the Ethical Standards issued by the UK Auditing Practices Board. As a result we have underlying safeguards in place to maintain independence through: Instilling professional values, Communications, Internal accountability, Risk management and Independent reviews.

We would be happy to discuss any of these aspects of our procedures in more detail.

Auditor declaration

In relation to the audit of the financial statements of Derbyshire Dales District Council for the financial year ending 31 March 2017, we confirm that there were no relationships between KPMG LLP and Derbyshire Dales District Council, its directors and senior management and its affiliates that we consider may reasonably be thought to bear on the objectivity and independence of the audit engagement lead and audit staff. We also confirm that we have complied with Ethical Standards and the Public Sector Audit Appointments Ltd requirements in relation to independence and objectivity.

Appendix 5

Audit fees

Audit fees

As communicated to you in our External Audit Plan 2016/17, our scale fee for the audit is £38,295 plus VAT *(£38,295 in 2015/16)*. However, we propose an additional fee of £2,000 due to additional work undertaken in relation to the CIES restatement. See table below for further detail.

Our work on the certification of Housing Benefits (BEN01) is planned for September 2017. The planned scale fee for this is £5,393 plus VAT.

PSAA fee table		
Component of audit	**2016/17** *(planned fee)* £	**2015/16** *(actual fee)* £
Accounts opinion and use of resources work		
PSAA scale fee set in 2014/15	38,295	38,295
Additional work to conclude our opinions (note 1)	2,000	0
Subtotal	**43,295**	**38,295**
Housing benefits (BEN01) certification work		
PSAA scale fee set in 2014/15	5,393	5,393
Total fee for the Authority set by the PSAA	**48,688**	**43,688**

All fees are quoted exclusive of VAT.

Note 1: Accounts opinion and use of resources work

For 2016/17, we have discussed additional fee in relation to CIES restatement with the S151 officer. This is still subject to PSAA determination.

BACK TO AGENDA

NOT CONFIDENTIAL – For public release Item No. 7

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Resources

STATEMENT OF ACCOUNTS 2016/17

SUMMARY

This report provides interpretation of the Statement of Accounts for 2016/17 and highlights the key issues. The Committee is requested to consider and approve the Statement of Accounts.

RECOMMENDATION

That the Statement of Accounts for 2016/17 is approved.

WARDS AFFECTED

All.

STRATEGIC LINK

The Council's financial position is taken into account in determining all the priorities in the Corporate Plan.

The financial position as at 31st March 2017 will be reflected in the review of the Council's Financial Strategy, which will be presented to the Council Meeting in November 2017, and in the revenue spending proposals for 2018/19, which will be presented in early 2018.

---

1. BACKGROUND

1.1 Under the Accounts and Audit Regulations 2015 the District Council must:-

- consider either by way of a Committee or by the Members meeting as a whole the Statement of Accounts;
- following that consideration, approve the Statement of Accounts by a resolution of that Committee or meeting;
- following approval, ensure that the Statement of Accounts is signed and dated by the person presiding at the Committee or meeting at which that approval was given; and
- publish (which must include publication on the Council's website), the Statement of Accounts together with any certificate, opinion, or report issued, given or made by the auditor.

2. REPORT

2.1 The Statement of Accounts 2016/17, distributed separately with this Agenda, has been audited by the Council's External Auditors, KPMG.

Some minor changes have been made to the Statement of Accounts in order to address issues identified during the audit. However, the overall financial position remains the same as that reported to Council on 22nd June 2017.

2.2 The Audit Opinion will be issued after the Committee has approved the Statement of Accounts and Letter of Representation. As part of corporate governance, the External Auditor is required to report relevant matters relating to the audit to the Committee. The External Audit Report 2016/17 from KPMG is included elsewhere on the Agenda of this meeting.

2.3 The Accounts and Audit Regulations state that the accounts must be prepared in accordance with "proper practices". The Local Government Act 2003 defines proper practices as those:

- Which the authority is required to follow by virtue of any enactment, or
- Which are contained in a code of practice or other document which is identified by the Secretary of State. The Secretary of State has determined that the following documents are relevant:

  - The Code of Practice on Local Authority Accounting in the United Kingdom 2015/16 (the Code), published by the Chartered Institute of Public Finance and Accountancy (CIPFA);
  - The Service Reporting Code of Practice (SeRCOP), published by CIPFA.

2.4 The Council's accounts have been prepared to comply with proper practices, as demonstrated by the satisfactory completion of the external audit of the accounts. Compliance can also be checked by reviewing the Statement of Accounts against the Audit Commission's Aide Memoire, which is included as Appendix 1 to this report.

3 RISK ASSESSMENT

3.1 Legal

Legal Considerations are contained within the body of the report. The legal risk is low.

3.2 Financial

The accounts have been prepared in accordance with proper practices, and have been audited. There is therefore no financial risk arising from this report.

4 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

5. CONTACT INFORMATION

For further information contact:

Karen Henriksen, Head of Resources, Telephone: 01629 761284
E-mail: karen.henriksen@derbyshiredales.gov.uk

6. BACKGOUND PAPERS

None

7. ATTACHMENTS

Appendix 1 – Statement of Accounts 2016/17 - Aide Memoire for Councillors

Appendix 2 – Statement of Accounts 2016/17 – Published Separately

APPENDIX 1

STATEMENT OF ACCOUNTS 2016/17- AIDE MEMOIRE FOR MEMBERS

The purpose of the questions below is to help establish and provide evidence of a robust review of the accounts by the S151 officer and Members.

No.	Issue	Members comment and evidence
1	Was the closedown plan (which allows the statement of accounts to be approved by members by 30 September 2016) achieved? Does this allow sufficient time for member review?	The accounts were signed by the S151 Officer on 11th September and sent to Members prior to Governance and Resources Committee on14th September.
2	Have the auditors received regular updates on the plan and been warned of potential problems?	The auditors received a copy of the plan in March. During the closure process discussions have been held with the auditors regarding various areas of accounting. The auditors were given a copy of the completed disclosure checklist and draft accounts at the commencement of the audit – the disclosure checklist helps them to identify potential problem areas.
3	Have staff preparing the accounts attended CIPFA/KPMG workshops and are they aware of the key issues and changes in the CIPFA Code of Practice 2016/17?	Yes. The Accountancy and Exchequer Manager and the Principal Accountant attended the KPMG Final Accounts Workshop.
4	Do staff preparing the accounts have up to date CIPFA guidance notes for practitioners?	Yes
5	Have the accounts been checked for casting errors, internal inconsistency and cross referencing? (All numbers which are expected to agree do agree).	Yes. Extensive use of Excel is incorporated into the document to reduce the risk of casting errors and to check internal consistency. Internal consistency and cross referencing is also checked thoroughly by senior accounting staff.

No.	Issue	Members comment and evidence
6	Does the narrative statement set out the results for the year and comparison to budget, commenting on the significant items? Do the figures quoted reconcile to the main statements?	Yes – see pages 1 to 8 of the draft Statement of Accounts. Yes.
7	Has the audit of the accounts been advertised and accounts made available for public inspection? Have members of the public raised any objections? (If so, what are they?)	Adverts were placed during the week ending 26th June 2017. The accounts were available for public inspection from 5th June to 14th July. No objections were received.
8	Has the disclosure checklist been completed in detail and sent, together with a set of the completed accounts, to the auditor as part of the accounts working papers protocol?	The auditors were given a copy of the draft accounts on 26 May 2017 and a copy of the completed disclosure checklist on 26th June 2017.
9	Has a bank reconciliation been completed as at 31st March 2017 with no unexplained entries?	Yes. The bank reconciliation for the year ending 31st March 2017 was completed on 18th April 2017. There were no unexplained entries.
10	Have all year-end control accounts been reconciled? How have you maintained control when staff are involved in budget preparations Nov – Feb time? Any significant slippages in reconciling suspense accounts e.g. cash suspense?	Yes. There were sufficient numbers of adequately training staff in the Financial Services Section (see risk register). No. Control and suspense accounts are reconciled at least quarterly. The cash suspense account is checked daily.
11	Are there any significant unexplained budget variances and latest forecasts?	No unexplained variances.
12	Have working papers been completed in accordance with the auditor's final accounts protocol? Were they ready for the start of the audit?	Working papers comply with the protocol, but were not fully completed for the commencement of the audit. This was due to some vacant posts and staff absences. It is hoped that all staff will be in post for the 2017/18 accounts closure process, including an additional Senior Accountant post that has recently been approved. An action plan for 2017/18 accounts will be agreed with the external auditors.

No.	Issue	Members comment and evidence
13	Is there a sufficient basket of evidence gathered to allow the S151 officer and members to conclude on the effectiveness of Internal Audit, in relation to the Annual Governance Statement? E.g. Self-assessment by Internal Audit Manager, External Auditor's view of Internal Audit, Heads of Service view of Internal Audit.	The Annual Governance Statement 2016/17, identifying the Governance Framework and a review of its effectiveness, was approved by the Governance and Resources Committee on 29th June 2017; The Internal Audit Annual Report was considered at the same meeting. This report includes an opinion on the overall adequacy and effectiveness of the Council's control environment including any qualifications to that opinion; The Internal Audit section is subject to regular inspection by the Council's external auditors, who place reliance on the work undertaken by the section.
14	Has the action plan from the previous year's Annual Governance Statement been complied with? Are there any remaining control risks that undermine the content of the Annual Governance Statement or the Accounts?	Progress on the action plan for the 2015/16 Annual Governance Statement is shown in the 2016/17 Statement, on page 28 of the Statement of Accounts. There were three recommendations relating to: • Financial pressures and achieving a sustainable budget; • Housing benefit overpayments; • Arrangements for data protection and information governance. The risks relating to housing benefit overpayments have been reduced following the introduction of improved arrangements. Outstanding actions relating to financial pressures and data protection arrangements have been carried forward to the 2016/17 action plan.

Prepared by Karen Henriksen, Head of Resources 18/08/2017.

BACK TO AGENDA

NOT CONFIDENTIAL – For public release **Item No. 8**

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Resources

LETTER OF REPRESENTATION 2016/17

PURPOSE OF REPORT

This report requests consideration of the draft Letter of Representation as part of their responsibility for approving the financial statements.

RECOMMENDATION

That the draft Letter of Representation is approved.

WARDS AFFECTED

All

STRATEGIC LINK

The Letter of Representation is an important aspect of the Council's corporate governance arrangements. As such, it contributes towards the achievement of all the Council's aims, priorities and targets.

---

1 REPORT

1.1 The International Standard on Auditing (U.K. & Ireland) 580 (ISA 580) requires the external auditor to obtain evidence that the Council's management acknowledges its responsibility for the fair presentation of the financial statements in accordance with the applicable financial reporting framework, and has approved the financial statements. The auditor can obtain evidence of management's acknowledgement of such responsibility by obtaining a written representation from management and a signed copy of the financial statements.

1.2 ISA 580 gives guidance on matters which might be included in a management "letter of representation". The Head of Resources' letter of representation has been prepared in accordance with that guidance and is given in Appendix 1. In preparing the letter, the Head of Resources has consulted with members of the Council's Corporate Leadership Team, and has discussed the draft contents with the External Auditor. The letter contains no matters of concern which need to be brought to the attention of Members.

1.3 In addition, ISA 580 requires the external auditor to obtain evidence that those charged with governance acknowledge their collective responsibility for the preparation of, and have approved, the financial statements. Approval of the letter of representation by the Governance & Resources Committee prior to receiving the external auditor's Annual Governance Report contributes to that evidence.

2 RISK ASSESSMENT

2.1 Legal

There are no legal risks arising from the report.

2.2 Financial

There are no financial risks arising from the report.

3 OTHER CONSIDERATIONS

In preparing this report the relevance of the following factors has also been considered: prevention of crime and disorder, equality of opportunity, environmental, health, legal and human rights, financial, personnel and property considerations.

4 CONTACT INFORMATION

Karen Henriksen, Head of Resources, Telephone: 01629 761284
Email: karen.henriksen@derbyshiredales.gov.uk

5 BACKGROUND PAPERS

International Standard on Auditing (UK & Ireland) 580 – Management Representations

6 ATTACHMENTS

Appendix 1 – Letter of Representation 2016/17

APPENDIX 1

DERBYSHIRE DALES DISTRICT COUNCIL

Mr J Cornett
Director
KPMG LLP
St Nicholas House
31 Park Row
Nottingham
NG1 6FQ

Please ask for: Karen Henriksen
Direct Dial No: 01629 761284
Your Ref.
My Ref. CE/KH
E-mail: karen.henriksen@derbyshiredales.gov.uk

15 September 2017

Dear John,

Derbyshire Dales District Council - Audit for the year ended 31 March 2017

This representation letter is provided in connection with your audit of the financial statements of Derbyshire Dales District Council ("the Authority"), for the year ended 31 March 2017, for the purpose of expressing an opinion:

i. as to whether these financial statements give a true and fair view of the financial position of the Authority as at 31 March 2017 and of the Authority's expenditure and income for the year then ended; and

ii. whether the financial statements have been prepared properly in accordance with the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2016/17.

These financial statements comprise the Expenditure and Funding Analysis, the Movement in Reserves Statement, the Comprehensive Income and Expenditure Statement, the Balance Sheet, the Cash Flow Statement and the Collection Fund and the related notes (including the Expenditure and Funding Analysis).

The Authority confirms that the representations it makes in this letter are in accordance with the definitions set out in the Appendix to this letter.

The Authority confirms that, to the best of its knowledge and belief, having made such inquiries as it considered necessary for the purpose of appropriately informing itself:

Financial statements

1. The Authority has fulfilled its responsibilities, as set out in the Accounts and Audit Regulations 2015, for the preparation of financial statements that:

i. give a true and fair view of the financial position of the Authority as at 31 March 2017 and of the Authority's expenditure and income for the year then ended; and

ii. have been prepared properly in accordance with the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2016/17.

The financial statements have been prepared on a going concern basis.

2. Measurement methods and significant assumptions used by the Authority in making accounting estimates, including those measured at fair value, are reasonable.

3. All events subsequent to the date of the financial statements and for which IAS 10 *Events after the reporting period* requires adjustment or disclosure have been adjusted or disclosed.

Information provided

4. The Authority has provided you with:

- access to all information of which it is aware, that is relevant to the preparation of the financial statements, such as records, documentation and other matters;
- additional information that you have requested from the Authority for the purpose of the audit; and
- unrestricted access to persons within the Authority from whom you determined it necessary to obtain audit evidence.

5. All transactions have been recorded in the accounting records and are reflected in the financial statements.

6. The Authority confirms the following:

i) The Authority has disclosed to you the results of its assessment of the risk that the financial statements may be materially misstated as a result of fraud.

Included in the Appendix to this letter are the definitions of fraud, including misstatements arising from fraudulent financial reporting and from misappropriation of assets.

ii) The Authority has disclosed to you all information in relation to:

a) Fraud or suspected fraud that it is aware of and that affects the Authority and involves:
   - management;
   - employees who have significant roles in internal control; or
   - others where the fraud could have a material effect on the financial statements; and

b) allegations of fraud, or suspected fraud, affecting the Authority's financial statements communicated by employees, former employees, analysts, regulators or others.

In respect of the above, the Authority acknowledges its responsibility for such internal control as it determines necessary for the preparation of financial statements that are free from material misstatement, whether due to fraud or error. In particular, the Authority acknowledges its responsibility for the design, implementation and maintenance of internal control to prevent and detect fraud and error.

7. The Authority has disclosed to you all known instances of non-compliance or suspected non-compliance with laws and regulations whose effects should be considered when preparing the financial statements.

8. The Authority has disclosed to you and has appropriately accounted for and/or disclosed in the financial statements, in accordance with IAS 37 *Provisions, Contingent Liabilities and Contingent Assets*, all known actual or possible litigation and claims whose effects should be considered when preparing the financial statements.

   There are no:

   - Other liabilities that are required to be recognised and no other contingent assets or contingent liabilities that are required to be disclosed in the financial statements in accordance with IAS 37 *Provisions, Contingent Liabilities and Contingent Assets*, including liabilities or contingent liabilities arising from illegal or possible illegal acts; or

   - Other environmental matters that may have an impact on the financial statements.

9. The Authority has disclosed to you the identity of the Authority's related parties and all the related party relationships and transactions of which it is aware. All related party relationships and transactions have been appropriately accounted for and disclosed in accordance with IAS 24 *Related Party Disclosures*.

   Included in the Appendix to this letter are the definitions of both a related party and a related party transaction as we understand them as defined in IAS 24 and the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2016/17.

10. The Authority confirms that:

    a) The financial statements disclose all of the key risk factors, assumptions made and uncertainties surrounding the Authority's ability to continue as a going concern as required to provide a true and fair view.

    b) Any uncertainties disclosed are not considered to be material and therefore do not cast significant doubt on the ability of the Authority to continue as a going concern.

11. On the basis of the process established by the Authority and having made appropriate enquiries, the Authority is satisfied that the actuarial assumptions underlying the valuation of defined benefit obligations are consistent with its knowledge of the business and are in accordance with the requirements of IAS 19 (revised) *Employee Benefits.*

    The Authority further confirms that:

    a) all significant retirement benefits, including any arrangements that are:
        - statutory, contractual or implicit in the employer's actions;
        - arise in the UK and the Republic of Ireland or overseas;
        - funded or unfunded; and
        - approved or unapproved,

    have been identified and properly accounted for; and

    b) all plan amendments, curtailments and settlements have been identified and properly accounted for.

12. The Authority has disclosed to you all information that should be included in the Annual Governance Statement that was approved by the Governance and Resources Committee and signed by the Leader of the Council and the Chief Executive on 29 June. The Authority confirms that there have been no circumstances that require an amendment to be made to the document between the date of signing and publication of the financial statements.

This letter was tabled and agreed at the meeting of the Governance and Resources Committee on 14 September 2017.

Yours sincerely,

Karen Henriksen

Head of Resources (Section 151 Officer)

Councillor J Stevens

Chairman of Governance and Resources Committee

Appendix to the Authority Representation Letter of Derbyshire Dales District Council: Definitions

Financial Statements

A complete set of financial statements comprises:

- A Comprehensive Income and Expenditure Statement for the period;
- A Balance Sheet as at the end of the period;
- A Movement in Reserves Statement for the period;
- A Cash Flow Statement for the period; and
- Notes, comprising a summary of significant accounting policies and other explanatory information and the Expenditure and Funding Analysis.

A local authority is required to present group accounts in addition to its single entity accounts where required by chapter nine of the CIPFA/LASAAC Code of Practice on Local Authority Accounting in the United Kingdom 2016/17.

A billing authority must present a Collection Fund Statement for the period showing amounts required by statute to be debited and credited to the Collection Fund.

An entity may use titles for the statements other than those used in IAS 1. For example, an entity may use the title 'statement of comprehensive income' instead of 'statement of profit or loss and other comprehensive income'.

Material Matters

Certain representations in this letter are described as being limited to matters that are material.

IAS 1.7 and IAS 8.5 state that:

“Material omissions or misstatements of items are material if they could, individually or collectively, influence the economic decisions that users make on the basis of the financial statements. Materiality depends on the size and nature of the omission or misstatement judged in the surrounding circumstances. The size or nature of the item, or a combination of both, could be the determining factor.”

Fraud

Fraudulent financial reporting involves intentional misstatements including omissions of amounts or disclosures in financial statements to deceive financial statement users.

Misappropriation of assets involves the theft of an entity’s assets. It is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorisation.

Error

An error is an unintentional misstatement in financial statements, including the omission of an amount or a disclosure.

Prior period errors are omissions from, and misstatements in, the entity's financial statements for one or more prior periods arising from a failure to use, or misuse of, reliable information that:

a) was available when financial statements for those periods were authorised for issue; and
b) could reasonably be expected to have been obtained and taken into account in the preparation and presentation of those financial statements.

Such errors include the effects of mathematical mistakes, mistakes in applying accounting policies, oversights or misinterpretations of facts, and fraud.

Management

For the purposes of this letter, references to "management" should be read as "management and, where appropriate, those charged with governance".

Related Party and Related Party Transaction

Related party:

A related party is a person or entity that is related to the entity that is preparing its financial statements (referred to in IAS 24 *Related Party Disclosures* as the "reporting entity").

a) A person or a close member of that person's family is related to a reporting entity if that person:
    i. has control or joint control over the reporting entity;
    ii. has significant influence over the reporting entity; or
    iii. is a member of the key management personnel of the reporting entity or of a parent of the reporting entity.

b) An entity is related to a reporting entity if any of the following conditions applies:
    i. The entity and the reporting entity are members of the same group (which means that each parent, subsidiary and fellow subsidiary is related to the others).
    ii. One entity is an associate or joint venture of the other entity (or an associate or joint venture of a member of a group of which the other entity is a member).
    iii. Both entities are joint ventures of the same third party.
    iv. One entity is a joint venture of a third entity and the other entity is an associate of the third entity.
    v. The entity is a post-employment benefit plan for the benefit of employees of either the reporting entity or an entity related to the reporting entity. If the reporting entity

is itself such a plan, the sponsoring employers are also related to the reporting entity.

vi. The entity is controlled, or jointly controlled by a person identified in (a).

vii. A person identified in (a)(i) has significant influence over the entity or is a member of the key management personnel of the entity (or of a parent of the entity).

viii. The entity or any member of a group of which it is a part, provides key management personnel services to the reporting entity or to the parent of the reporting entity.

Key management personnel in a local authority context are all chief officers (or equivalent), elected members, the chief executive of the authority and other persons having the authority and responsibility for planning, directing and controlling the activities of the authority, including the oversight of these activities.

A reporting entity is exempt from the disclosure requirements of IAS 24.18 in relation to related party transactions and outstanding balances, including commitments, with:

a) a government that has control, joint control or significant influence over the reporting entity; and
b) another entity that is a related party because the same government has control, joint control or significant influence over both the reporting entity and the other entity.

Related party transaction:

A transfer of resources, services or obligations between a reporting entity and a related party, regardless of whether a price is charged.

BACK TO AGENDA

NOT CONFIDENTIAL – For public release **Item No. 9**

GOVERNANCE & RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Corporate Services

COMMUNICATIONS AND MARKETING STRATEGY

SUMMARY

The Communication and Marketing Strategy sets out how residents, employees and service users are kept informed about what the District Council is doing, how it is spending public money, and the District Council services they can access.

RECOMMENDATIONS

1. That the strategic framework of the current Communications and Marketing Strategy is noted.

2. That the action plan for 2017/2018 is approved.

3. That a supplementary revenue estimate is approved in the sum of £5,000 to enable the signage works to be completed in 2017/18.

WARDS AFFECTED

All

STRATEGIC LINK

Good communications with residents, employees and service users is key to all the District Council's corporate priorities and pivotal to providing excellent services.

---

1 BACKGROUND

1.1 The District Council adopted its current Communications and Marketing Strategy in September 2014, reflecting the development of technology and the needs both of the public and the District Council, which had evolved dramatically since the previous strategy's adoption in 2011. This third annual update sets ambitious yet realistic targets to support the Council's Corporate Objectives and core values.

1.2 The aim of the Strategy is to ensure our communications help to promote a positive image of the Council, and, in marketing terms, help us to meet the needs and wants of our customers in a fast moving digital world.

1.3 The adopted Strategy sets out a multi-channel approach to reach a wide variety of customers and stakeholders, underlining traditional forms of communication while embracing more modern approaches.

1.4 Communicating well is the responsibility of everyone and the Strategy is designed to be a useful tool for the corporate leadership team, heads of services and all employees and elected members. It sets a framework for communications and gives direction to all media, online, internal, marketing, publications and public relations communications actively undertake on behalf of the district council.

1.5 The Communications and Marketing Strategy sets out ways to:

- Make the Council easy to understand and talk to
- Co-ordinate and direct communications
- Ensure that everyone understands our targets and what the outcomes will be
- Ensure that staff and partners understand their contribution
- Make sure people know the outcome of the changes the District Council makes
- Ensure openness and transparency
- Make people feel better informed, proud to live in Derbyshire Dales, proud to work for the Council and proud to work with it.

1.6 The Strategy (attached as Appendix 1) is without a timeframe. This is deliberate and seeks to set a strategic framework with a more dynamic approach to actions which can be measured by way of an Annual Action Plan, monitored by a Communications & Marketing Hub comprising officers from all Council service areas.

2 REVIEW OF 2016/17 ACTION PLAN

Internet

2.1 *Enhance the District Council's reputation by upgrading and improving signage across the district*

The first phase of this project is almost complete, with new signage costed and designed for the welcome signs on main routes on the district's borders, at the Town Hall and in our parks and gardens. A second phase is now proposed (see 3.1)

Website visitors

2.2 *Drive website monthly visitor numbers from 63,130 to 70,620*

After increasing visitor number by almost 10% in 2015/16, the last year has been a challenge due to the number of established Google links we deliberately "broke" in relaunching our new mobile-friendly website in March 2016, where we changed the menu structure to make it more intuitive. In the months following the relaunch visitor numbers actually reduced, but, with the gradual re-establishment of links, we are now back on track and, although below target, the average number of monthly visits has increased during the

past year by 3.35% to 65,920. Note: the number of visits increased by 33% from June-August 2017.

Twitter feed

2.3 *Increase followers on our corporate Twitter feed from 5,620 to 6,463*
After increasing the number of people who follow our Twitter feed by 25% in 2015/16, it was noted when setting the past year's target that there would be an inevitable slow-down in new followers as we started to reach saturation point. The good news however is that we have hit our 15% target increase.

Facebook

2.4 *Increase the number of 'Likes' across all District Council Facebook pages from 17,850 to 20,527*
We went for a 15% increase on followers across our 11 Facebook pages and over-achieved in the past year, reaching a total of 25,610 follows.

e-Newsletter

2.5 *Increase e-newsletter database names and addresses from 2,850 to 3,277*
The actual figure today is 3,505 names

Media training

2.6 *Continue to support members and managers with media training*
All new members were invited to attend media training after the May 2015 elections and this training has been extended to departments

Media releases

2.7 *Issue a minimum of two media releases every week* - Not as significant a tool in the communications kit as it formerly was, but we have issued ?? releases in the year to date, so are on target

Licences

2.8 *Ensure all leases and licences include District Council branding by condition to enhance the authority's reputation*
We continue to police this requirement

SMS

2.9 *Utilise SMS effectively for corporate, promotional and internal use*
We have acquired an SMS tool in the past year that enables us to quickly send alerts to staff colleagues in the event of bad weather etc, but this has not yet been developed for corporate or promotional use after the project was put on hold by the council's Transformation Team.

New social media channels

2.10 *Investigate and introduce new social media channels such as Instagram to further extend the reach of our communications*
In the past year we've launched a corporate Instagram page and separate pages for leisure and Matlock Bath Illuminations, resulting in a total of 400 followers. Being photo-led, Instagram is a nice-to-have reputational tool, but doesn't give us the promotional flexibility of Facebook and Twitter.

Corporate identity

2.11 *Review the corporate identity guide to ensure it is fit for purpose in the 21st century*

The signage project has to some extent informed this action point in the past year, but more work needs to be done in the coming year.

Customer satisfaction

2.12 *Enable a survey that investigates the overall level of satisfaction in the District Council*

We have enabled a number of customer surveys in the past year and have direct access to an online panel via our Mailchimp email database comprising more than 700 residents

Video

2.13 *Increase use of video to improve democracy/accountability of council meetings and to increase engagement across our digital media platforms*

All full council meetings and high profile special meetings are now live streamed on the council's YouTube channel working to a relatively low-cost specification developed by the Communications Manager and Business Support Supervisor Ian Brailsford. Where other authorities have invested heavily (and expensively) in streaming infrastructure, we have put together an inexpensive multi-camera mix that can be operated, if necessary, by just one member of staff. Additionally, we use video for internal messages to all staff from the Chief Executive and our leisure centres are increasingly using the Facebook Live facility to promote fitness classes etc.

Community Development marketing

2.14 *Community Development marketing target - to increase 'Likes' across our leisure centres' social media channels (Facebook and Instagram) by 15%*

Arc Leisure Matlock and Ashbourne Leisure Centre have made huge strides in the past year making their Facebook pages more engaging and have easily exceeded the 15% target. The leisure Instagram page remains ripe for further development however.

3 NEW ACTION PLAN, 2017/18

The big issue for the next Action Plan is once again allocating a sum from the communications budget set aside annually to improve the reputation of the District Council. This amount was £12,000 in the year to date, but is reduced to £5,000 for the coming year to September 2018. In previous years, in addition to the signage project, we have updated the website and the design of Dales Matters.

The Communications & Marketing Hub, which has Councillor Pawley as Member Representative, has agreed that in the coming year we need to continue to address the issue of signage in a second phase. It was not be possible to achieve all our ambitions within the 2016/17 budget, and our wish-list for the coming year would include:

- pursuing sponsorship opportunities, especially for our new boundary signs
- introducing signage to the remaining 20 smaller parks and gardens (this is happening in 10 smaller parks and gardens in phase one)
- introducing statement signs in our larger parks
- reviving memorial plaque sponsorship of park benches in liaison with the Environmental Services service area
- reviewing generally the ad hoc nature of signage in our parks and introducing improvements

A supplementary revenue estimate is requested for approval in the sum of £5,000 to enable the signage works to be completed at a total additional cost of £10,000.

The full Action Plan would look like this:

3.1 Enhance the District Council's reputation by upgrading and improving signage across the district in a second phase of this project

3.2 Make SIDD fully available to staff and Members externally, transferring the current Members' Portal to an improved platform on SIDD

3.3 Support members and managers with new presentational and social media training

3.4 Increase e-newsletter database names and addresses from 3,505 to 3,855 (+10%)

3.5 Issue a minimum of two media releases every week

3.6 Ensure all leases and licences include District Council branding by condition to enhance the authority's reputation

3.7 Review the corporate identity guide to ensure it is fit for purpose in the 21st century

3.8 Utilise our online panel to gauge the overall level of satisfaction in the District Council

3.9 Continue to use video to improve democracy/accountability of council meetings and to increase engagement across our digital media platforms

Communications and Marketing Hub Member Representative **Councillor Joyce Pawley** will report verbally to the Committee.

4 RISK ASSESSMENT

4.1 Legal

An effective communications strategy helps to reinforce the District Council's ambition and raises proper accountability. The Strategy has been framed within the legislative framework regarding publicity. The legal risk is therefore low.

4.2 Financial

The Communications Strategy can be delivered within existing budgets and, therefore, the financial risk arising from this report is low.

5 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

6. CONTACT INFORMATION

Jim Fearn, Communications and Marketing Manager on 01629 761195 or email *jim.fearn@derbyshiredales.gov.uk*
Sandra Lamb, Head of Corporate Services Tel. 016289 761282 or email sandra.lamb@derbyshiredales.gov.uk

7. BACKGROUND PAPERS

None

8. ATTACHMENTS

Communications and Marketing Strategy (updated September 2016)




Communications & Marketing Strategy


CONTENTS

Derbyshire Dales District Council

Communications & Marketing Strategy

(Adopted, Corporate Committee, 18 September 2014)

(New action plan to Governance & Resources Committee, 17 September 2015)

Introduction

Communication plays an important role in everything we do at Derbyshire Dales District Council.

Communicating **well** is the responsibility of everyone at the District Council, not just the communications team. This strategy is designed to be a useful tool for the corporate management team, heads of services, all employees and council members.

It sets a framework for district council communications and gives direction to all media, online, internal, marketing, publications and public relations communications activity undertaken on behalf of the district council.

Our commitment is to use a **multi-channel approach** to reach the wide variety of customers and stakeholders we serve, including residents, employees, businesses, community partners, visitors to the district and all levels of government.

Externally, a key focus is to promote the district council's services to give us a competitive edge, supporting and enhancing regular activities.

Internal communications will involve all staff in shaping services as the district council continues to go through major changes.

We will seek to provide communications services on the most cost-effective basis, for example by accelerating our shift towards digital communications and taking a “digital first” position on crisis management

We will commit to continuing improvement of the usefulness of our website and keep content fresh and updated as we move a greater share of our communications activity online, utilising free social media channels.

Communication works best when it is a two-way process (we need to listen as well as talk) and when messages are clear and easy to understand. Our social media channels (particularly Facebook and Twitter) provide a voice for local people to air their views and discuss issues with the council.

The challenge for an organisation with more than 100,000 customers and a large range of services is how it communicates clearly and simply in a complex and constantly changing environment, with ever increasing financial pressures. This strategy seeks to address that challenge.

Research shows that communication with residents is a key driver to overall satisfaction with council performance. It is also at the heart of good customer service and effective, meaningful consultation – and critical to delivery of the council's role in the community.

This strategy sets out the framework within which we can respond to this challenge.

Aims, Vision and Objectives

Aims

The ultimate aim of our communications is that all staff, residents, partners and everyone who deals with the council will have a clear understanding and a positive perception of our vision, aims, values, services and achievements, leading to higher levels of satisfaction and engagement.

Vision

What are we trying to do?

To make its vision come alive, the district council must be able to communicate with (and influence) a wide range of organisations, individuals and partners.

We therefore need to …

- make the council easy to understand and talk to
- coordinate and direct communications so that all parts of the district council are working towards shared objectives, in support of council strategy
- ensure that everyone understands our targets, and what the outcomes will be – showing people what success looks like
- ensure staff and partners understand their contribution through clear objectives, milestones and deadlines
- make sure people know the outcome of the changes the district council makes
- ensure openness and transparency
- make people feel better informed, proud to live in Derbyshire Dales, proud to work for the council, and proud to work with it.

In other words, we need to continue to build the district council as *a brand*.

The visual element of this brand – our corporate identity – is generally understood by staff and customers. Our brand is an important communications tool, *made up of these components…*

- Our overall purpose – what are we here for?
- Our values – what drives us to do the things we do?
- Our key messages – what are we saying about what we offer?
- Our service delivery – what do we provide, compared with what we promise?
- Our behaviour – how do we treat our customers and our staff?

It is important we bring these elements together in a unified approach across all communications channels, so that we are consistent in tone, look and feel. People need to understand who we are and what we stand for.

In this, our Communications Strategy will dovetail with the council's Customer Access Strategy.

Objectives

- To secure and strengthen the reputation of the council in the community and an effective and efficient provider of high quality outcomes - focused on our values and priorities
- To build and maintain a professional corporate identity for consistent and co-ordinated use throughout the organisation
- To promote the image of the council as an effective, efficient and listening organisation focused on the public and their needs
- To ensure that communications are consistent and co-ordinated across all channels to give maximum support to the council's strategic priorities
- To ensure all staff understand the priorities of the council and feel valued and able to contribute to major changes affecting services they provide
- To ensure that our communications activities reflect the full diversity of the community and help ensure equality of access to all our services.

It is important also that the district council increases its efforts to understand what local communities are saying.

This strategy will dovetail with our Consultation Strategy in sharing information gained through consultation programmes such as citizens' panel consultation, channel shift

initiatives and increasing use of new technology devices to generate instant feedback on topical issues.

Delivering our objectives

The district council's reputation is based on perceptions – how people see us. Managing our reputation means first of all understanding what those perceptions are, deciding how we want to be seen, and planning how to get there.

We will tackle this by focusing internal capacity on the district council's key messages and ensuring that the most appropriate level of resource is available for our key priorities and activities.

Our communications platforms can be broken down into three:

- Traditional Media, Publications, Campaigns and PR
- Digital Media
- Internal Communications

Traditional Media, Publications, Campaigns and PR

We will seek to maintain and further improve positive media coverage and develop our media relations service to promote and defend the council, recognising the proven link between the public's sense of feeling informed and feeling satisfied. Our target is to issue two positive **media releases** every week of the year, alongside, where possible, engaging photography (chiefly taken in-house).

DERBYSHIRE DALES DISTRICT COUNCIL

Town Hall, MATLOCK, Derbyshire DE4 3NN
Tel: 01629 761100

PRESS RELEASE (with photo)
13 October 2014 - for immediate release

2014/081

Getting a kick out of latest sporting craze

Derbyshire Dales District Council is making sure local over 50s get a kick out of the latest sporting craze - walking football!

Weekly sessions of a game that has all the same rules as football - but with no running - are being organised in Baslow and Matlock, costing just £3 a time.

The first - at Baslow's newly refurbished multi-games area, is on this Thursday (16 October) from 10-11am. Wednesday morning sessions will take place at the District Council's Arc Leisure Matlock from 22 October, again from 10-11am.

The District Council is working in partnership with Derbyshire FA and Village Games, and Chairman of the District Council's Community Committee, Councillor Jennifer Bower said: "Walking football has suddenly grown from nothing to become the latest craze and we're delighted to offer sessions not only for over 50s, but for local people recovering from injuries."

There is no need to book in advance, but for more information contact the District Council's Village Games co-ordinator Becky Bryan on 01629 761385 or email rebecca.bryan@derbyshiredales.gov.uk

ENDS

For more information please contact: Jim Fearn on 01629 761195, e-mail: jim.fearn@derbyshiredales.gov.uk

It will also be the responsibility of the communications team to handle a communications problem or bundle of problems by identifying:

- the nature of the problem or challenge
- the key considerations in addressing it
- the key drivers of those decisions (crucially, insight into audiences)
- the resources required
- the stages to go through

We will issue reactive statements to media on request after gaining advice and approval first from the head of service (corporate management team member) and/or council leaders.

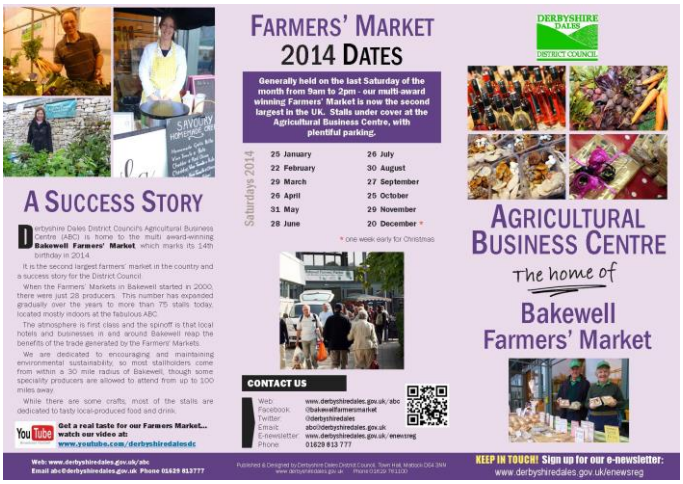
Despite our increasing focus on e-communications channels, the twice-yearly **dalesMATTERS** newsletter, delivered to all 33,000 homes in the district, remains an important communications tool. 90% of our citizens' panel (surveyed November 2013) had seen a copy of dalesMATTERS and 75% read half or most of it.

We will continue to edit, design and organise publication and distribution of dalesMATTERS, directed by an editorial panel comprising a representative from every service area.

Similarly, we will edit, design and organise publication of other special publications such as:

- Council Tax information leaflet

- Agricultural Business Centre annual leaflet (including Bakewell Farmers' Market dates)
- Community Safety newsletter (twice yearly)
- Various leisure publications
- Other leaflets and fact sheets (including an A-Z of council services)



We will maintain and develop our programme of media and integrated **campaigns** that underpin the district council's values and priorities.

We will use no/low-cost external sites such as poster frames in our pay & display car parks and public toilets to promote our services, including:

- Leisure centres
- Markets
- Parks and open spaces
- Special events such as our Matlock Bath Illuminations
- Do it online campaigns (channel shift)

The communications team, in consultation with the head of corporate services, will regularly change the organisation's **corporate email sign-off** as another channel to promote ongoing campaigns.

We will continue to evaluate and cost the potential of paid-for media (including local commercial radio stations and newspapers/magazines) to further promote our campaigns.

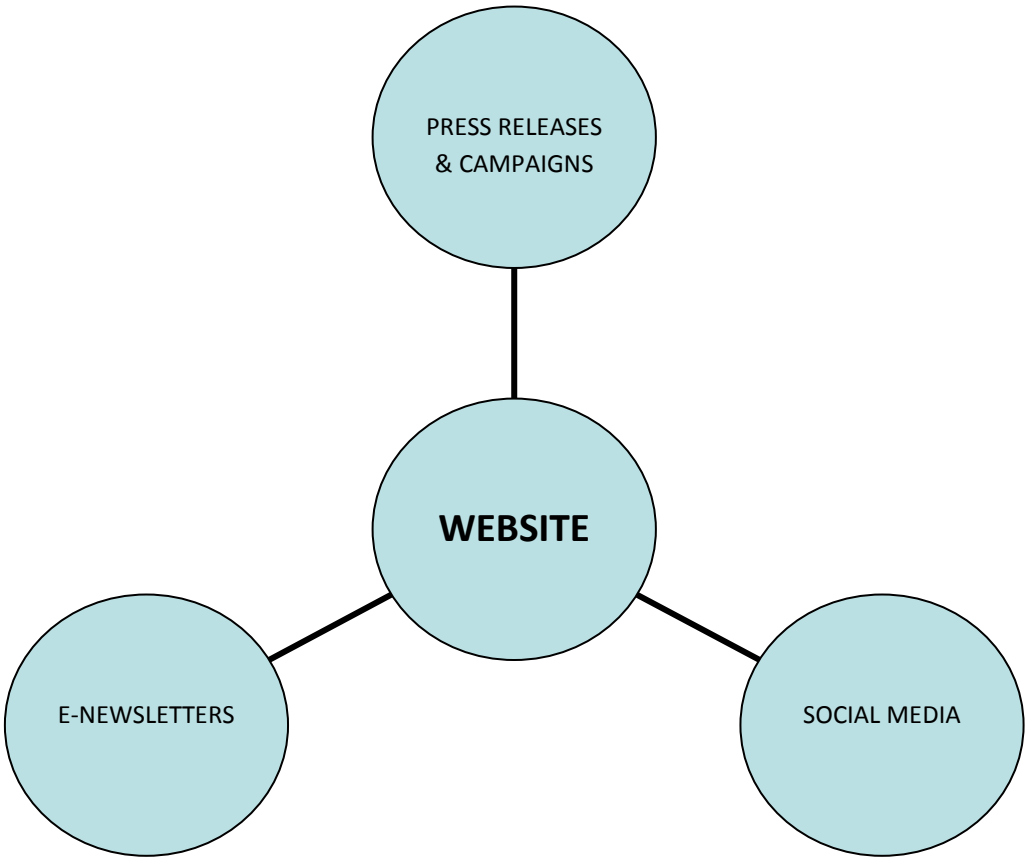
Digital Media

We recognise the value of our website as a source of information, as a point for customer transactions and as a low-cost alternative to face-to-face and telephone contact.

Our communications going forward will have a digital focus, building on the platform created by our website, relaunched in 2012 using an open source (Joomla) content management system to serve the public and businesses of Derbyshire Dales.

We will further develop the website to make it even easier to find the information you need, to report faults and incidents, to ask questions and to conduct many different types of transactions, all in a 24/7 environment.

Not only is this usually faster than alternative methods of contact, it means you can conduct your business with the district council when and where you like, while doing so at a lower cost to the taxpayer. We will aim to further increase use of the website, which currently attracts more than 40,000 visits every month and is the "hub" of our communications.



We are committed to continuing to improve visitor numbers and the accessibility of the website, creating new web forms and payment portals.

We are applying the same principles to the development of a new intranet site for staff (launched autumn 2014).

Social media platforms have become an integral part of our communications strategy. We recognise the opportunities that social media can deliver in terms of reputation enhancement, engaging with the public using their medium of choice, greater two-way dialogue and the insights that social media can provide, and as an opportunity to reduce cost versus other communications channels.

We will exploit the penetration of social media in dealing with crisis communications, providing regular news updates on our digital channels to create a channel shift away from phone calls to service centres during busy periods.

While operating and monitoring established Facebook, Twitter, Instagram and YouTube channels, we will examine the potential of other social media platforms. District council service areas will be assisted in setting up their own social media channels on request.

We will continue to use social media management tools such as Hootsuite to monitor our own social media activity and also gain a better understanding of the conversations about us in which we are not currently participating.

In parallel with the development of this Communications Strategy, we will continue to promote and, where necessary, update, our social media policy and staff guidelines.

We will seek to build our **e-newsletter** (MailChimp) database, enabling us to target key messages on a regular basis to engaged people in our communities. We recognise the huge potential of e-newsletters as an effective communications channel

Internal communications

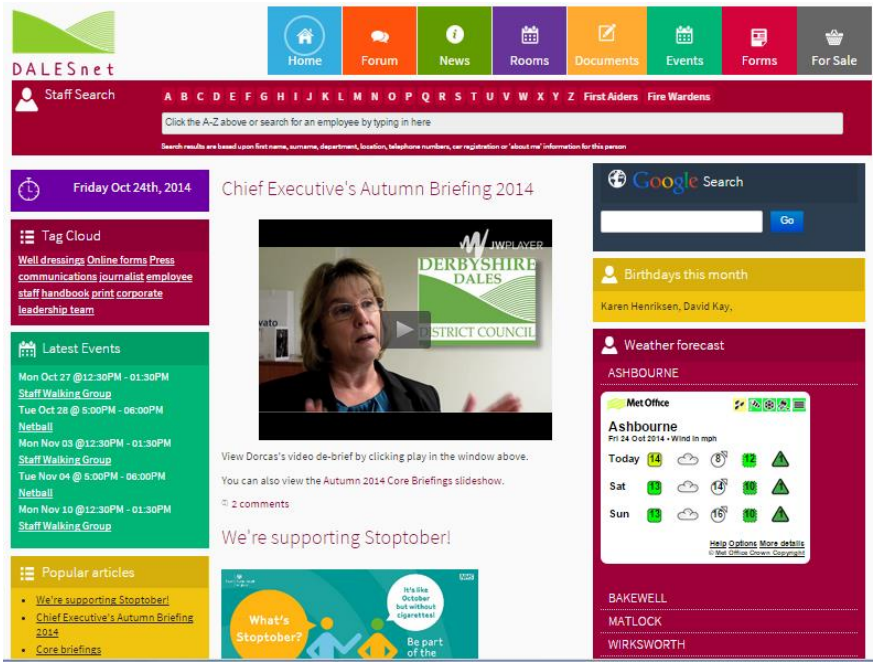
Internal communications play a key role in ensuring staff keep in touch with the district council's plans and priorities, and the challenges ahead.

Employees need to understand how their actions contribute to the overall achievement of priorities and how their behaviour affects the way the organisation is perceived internally and externally.

Our internal communications will include:

- Publication of the staffMATTERS internal newsletter, published six times a year
- A new (autumn 2014) more accessible intranet site

- An online forum where staff can advertise activities and events (internal and external) and suggest good ideas
- Regular all-staff emails
- In-house posters
- Screensaver messages on staff PCs
- Core briefings **videos** to get our messages across



Through all the channels listed above, we will support our consultation teams in their work to help the district council understand what the public truly want, to deliver on our values and priorities and to provide the best possible value for money.

Looking ahead

A Peer Review carried out in 2013 helped the district council re-set its vision – which is to use the reduced resources available to us more efficiently to maintain and - where possible - improve the quality of life for Derbyshire Dales people. A key aim of our communications is to help local people understand the financial challenges faced by the district council and the hard choices it is having to make in terms of service delivery.

Our plans are built on clear **values** that will help to steer us through the years ahead. Applying these values will mean that the district council is not only smaller, but also more flexible and more responsive to local people's needs and expectations.

We value:

- the uniqueness of our communities, businesses and residents
- working in partnership to deliver affordable, quality services
- our employees
- teamwork, working together across the organisation
- creative thinking and ambition

Supporting our values:

- the Council will be open and transparent when making decisions and will use public resources ethically and responsibly.

- we will behave with integrity, courtesy and respect, listening and responding to the very best of our abilities and treating everybody fairly, and by encouraging Members and staff to deliver improvements through their own personal development.

Providing the basics

In the coming years, we will have less money and will have to make sure we spend it where the need is greatest. Our role is to make sure local people get good outcomes from their services and we understand that it is the quality of the service that matters to local people, not who provides it.

Our focus should be on:

Promoting and regularly reinforcing the distinctive qualities both of the Derbyshire Dales and the district council. It is appropriate therefore to build communications skills across the organisation, supported by an in-house communications resource that is empowered to identify and solve communications problems, and resourced to implement solutions.

Helping communities help themselves

The district council is at its most effective when it is helping people to live successful lives as independently as possible and helping communities to help themselves. We believe that if power is in the hands of local people, you get better results and achieve better value.

Our approach will be to:

- Give individuals more say about the services they receive and the support they receive

- Empower communities to do more themselves and give them the tools they need for community action

- Recognise that some areas need more help than others and that, with a little support, they can get their ideas off the ground
- Support the transfer of buildings and other assets to community ownership so that they can become a hub for local activity – flexible and responsive to local needs.

Evidence and analysis

What do our customers and stakeholders say?

We continue to invite customers and stakeholders to help us set some key priorities that support our values. Research (notably through our most recent citizens' panel survey – November 2013) has revealed the following as our customer and stakeholder priorities:

1. Housing which meets local needs

Increase the availability of affordable housing for vulnerable people

2. A clean, green and prosperous Dales

Minimise waste and increase recycling. Enable development sites and business growth.

3. Safe and healthy communities

Keep alcohol-related crime low. Encourage active and healthy lifestyles.

Action Plan 2016/17

- Enhance the District Council's reputation by upgrading and improving signage across the district
- Drive website monthly visitor numbers from 63,130 to 70,620
- Increase followers on our corporate Twitter feed from 5,620 to 6,463
- Increase the number of 'Likes' across all District Council Facebook pages from 17,850 to 20,527
- Increase e-newsletter database names and addresses from 2,850 to 3,277
- Continue to support members and managers with media training
- Issue a minimum of two media releases every week
- Ensure all leases and licences include District Council branding by condition to enhance the authority's reputation
- Utilise SMS effectively for corporate, promotional and internal use
- Investigate and introduce new social media channels such as Instagram to further extend the reach of our communications
- Review the corporate identity guide to ensure it is fit for purpose in the 21st century
- Enable a survey that investigates the overall level of satisfaction in the District Council
- Increase use of video to improve democracy/accountability of council meetings and to increase engagement across our digital media platforms
- Community Development marketing target - to increase 'Likes' across our leisure centres' social media channels (Facebook and Instagram) by 15%

BACK TO AGENDA

NOT CONFIDENTIAL – For public release Item No. 10

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Community Development

CCTV DATA PROTECTION AND COMPLIANCE

PURPOSE OF REPORT

To ensure compliance with the impending introduction of the General Data Protection Regulation including additional resources required to manage the District Council's CCTV system.

RECOMMENDATION

That Council be recommended to approve expenditure of £11,100 from the General Reserve be approved to enable an increase in working hours for the current CCTV Manager.

WARDS AFFECTED

Not applicable

STRATEGIC LINK

Contributing to the District Council's aims for a clean, safe and thriving environment, District and community by keeping public places safe, tackling crime & anti-social behaviour.

---

1. REPORT

1.1 The introduction of the General Data Protection Regulation in May 2018 created additional requirements around the management of the District Council's CCTV System. These are mainly focused on how the authority needs to respond to people who request CCTV data.

1.2 The District Council is not currently equipped to deal with the new requirements and following the recommendation by the Data Protection Consultant, additional resource will be required for this.

1.3 An increase of 2 days per week to the CCTV manager's contract for a period of 12 months is requested to help meet these requirements.

1.4 The cost of this is approximately £11,100 and as there is no budgetary provision available within the service. Funding is therefore requested from the General Reserve.

1.5 The effectiveness of the extended contract will be monitored and reviewed towards the end of the 12 month period. If it is felt that an extension of the contract is necessary, further funding may be requested.

1.6 Without this role it is expected that the District Council will not be able to fully resource usage of the CCTV system and would struggle to deal with disclosure requests from both partner organisations and members of the public.

1.7 The General Data Protection Regulation does not allow charges for footage requests, therefore this means there will be no option to recover costs to be levied.

2. RISK ASSESSMENT

2.1 Legal

The legal risk has been assessed as low. The Council's Framework for Corporate Governance requires the Council to put in place effective arrangements for an objective review of risk management and internal control. Increasing the hours for the CCTV Manager will assist the Council in resourcing the effective monitoring of the CCTV system and its ability to respond to disclosure requests.

2.2 Financial

The request for additional funding from the General Reserve is for Council to decide, should the committee agree with the need. The financial risk is however low.

OTHER CONSIDERATIONS

In preparing this report the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

CONTACT INFORMATION

Ashley Watts, Head of Community Development
Tel: 01629 761367
Email: ashley.watts@derbyshire.dales.gov.uk

Karen Cooper, Community Safety Officer
Tel: 01629 761187
Email: karen.cooper@derbyshiredales.gov.uk

NOT CONFIDENTIAL – For public release Item No. 11

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Resources

INFORMATION SECURITY POLICY

PURPOSE OF REPORT

To seek approval for the 2017 revision of the Information Security Policy.

RECOMMENDATION

That the updated Information Security Policy is approved.

WARDS AFFECTED

None

STRATEGIC LINK

The Information Security Policy contributes to the delivery of all corporate priorities.

---

1 REPORT

1.1 The Council's Information Security Policy is developed by the Joint ICT Service, with the intention that the same policies will apply to all three Councils, Derbyshire Dales District Council, Bolsover District Council and North East Derbyshire District Council. This ensures a consistent approach across the joint ICT service, which is more efficient.

1.2 The current Joint Information Security Policies were developed in 2014, approved in 2014 and are now due for review. The original policy set was based on draft policies developed by the Local Government Association and a group of Councils. Its aim was to satisfy the compliance requirements of what is now known as the Public Service Network (PSN).

1.3 The key changes in relation to the 2017 revision are:

- Reference to and adoption of the new Government Security Classification Scheme;
- Improved clarity of key messages;
- Removal of duplication.

1.4 The updated policy is shown in Appendix 1. It includes the Joint Information Security Policy and a number of Appendices which provide greater detail and guidance around specific use.

2 RISK ASSESSMENT

2.1 Legal

Having a set of comprehensive Information Security polices support the Council's responsibilities against Public Service Network(PSN) compliance, the Computer Misuse Act, Data Protection Act and the forthcoming General Data Protection Regulations. The legal risk has been assessed as low.

2.2 Financial

There is no cost in implementing the updated polices. However, implementation can mitigate the risk of breaches of legislation and associated fines and reputational damage. The financial risk is therefore assessed as low.

4 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

5 CONTACT INFORMATION

Karen Henriksen, Head of Resources
Telephone: 01629 761284; Email: karen.henriksen@derbyshiredales.gov.uk

Nick Blaney, ICT Manager
Telephone: 01246 217097; Email: nick.blaney@ne-derbyshire.gov.uk

6 BACKGROUND PAPERS

None

7 ATTACHMENTS

Information Security Policy (September 2017)

Derbyshire Dales District Council,

INFORMATION SECURITY POLICY

June 2017

CONTROL SHEET FOR Information Security Policy

Policy Details	Comments / Confirmation (To be updated as the document progresses)
Policy title	Information Security
Current status – i.e. first draft, version 2 or final version	Draft
Policy author(s)	ICT Manager
Location of policy – i.e. L-drive, shared drive	Within IT area on X:
Member route for approval	Committee
Cabinet Member (if applicable)	
Equality Impact Assessment approval date	May 2013
Partnership involvement (if applicable)	
Final policy approval route i.e. Executive/ Council /Planning Committee	Committee
Date policy approved	
Date policy due for review (maximum three years)	2020
Date policy forwarded to include on Intranet and Internet if applicable to the public	

Contents

1 Introduction

In order to ensure the continued delivery of services to our customers Derbyshire Dales District Council are making ever increasing use of Information and Communication Technology (ICT).

The information that the Council holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected.

In order to maintain public confidence and ensure that the district Council comply with relevant statutory legislation, it is vital that the Council maintain the highest standards of information security. As such, a number of policies are in place to maintain these high standards of information security; these are attached as appendices to this summary document.

2 Scope

The policies applies to all users, the definition of users within this policy is intended to include all Services, partners, employees of the Council and other stakeholders such as contractual third parties, agents, work placements, where they have access to ICT facilities.

These policies are produced in line with guidelines and legislation that are available as of February 2017. These include:

2.1 Legislation and guidelines:

Copyright, Designs and Patents Act 1988 – downloading, copying, processing or distributing information from the internet may be an infringement of copyright or other intellectual property rights.

Data Protection Act 1998 and, from May 2018, the General Data Protection Regulations– care should be taken in the collection, processing or disclosure of any personal data and all personal data should be processed within the principles of the Act.

Information Commissioners Office (ICO) General Data Protection Regulations Guidance 1.0. This expands on the Data Protection Act

Human Rights Act 1998 – The HRA provides for the privacy of personal correspondence and the protection of that privacy while at work. Monitoring unless notified and done properly may infringe these rights

Freedom of Information Act 2000 – all recorded information is potentially disclosable under the Act, including all expressions of fact, intent and opinion. If a request for information is made, the Act prohibits destruction of the information until it is given out

in response to the request. Please also see the Council guidelines on retention of information.

Local Public Services Data Handling Guidance covers Central Government produced data and documents and is now being adopted more widely.
See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370725/PSN_local_public_services_data_handling_guidelines.pdf

Public Services Network (PSN) Code of Connection. This is a requirement to access central government provided services and a comprehensive list of conditions must be met to achieve the requisite compliance.

3 Principles

This document provides a summary of the information security policies developed by the Council. The objective of these policies is to ensure the highest standards of information security are maintained across the Council at all times so that:

- Duties are carried out in a professional and lawful manner and in accordance with the Council Codes of Conduct.
- The public and all users of the Council information systems are confident of the confidentiality, integrity and availability of the information used and produced.
- Business damage and interruption caused by security incidents are minimised.
- Customer and employee data is adequately protected and the risk of data protection breaches reduced.
- All legislative and regulatory requirements are met.
- The Council ICT equipment and facilities are used responsibly, securely and with integrity at all times.

The guidelines aim to set out the Council policy on the use and monitoring of ICT and seek to strike a balance between users' right to privacy and the Council responsibility to ensure appropriate use of ICT.

Failure to comply with these guidelines may be viewed as a disciplinary matter and may, therefore, be subject to the Council agreed Disciplinary Procedures.

It is intended that from time to time, as is required by changes to legislation, technology or the Council' policy, these Guidelines will be subject to review. Any changes made will be subject to consultation and the changes communicated to users. By signing the agreement users are deemed to accept any revisions to this policy that are communicated to them.

4 Risks

Derbyshire Dales District Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. This policy aims to mitigate those risks.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide services to our customers**.**

5 Information Security Policy

The key areas of this policy are detailed below:

- Protective Marking Policy
- Email Policy (Appendix 1)
- Internet Acceptable Usage Policy (Appendix 2)
- Software Policy (Appendix 3)
- ICT Access Policy (Appendix 4)
- PSN Acceptable Usage Policy and Personal Commitment Statement (Appendix 5)
- Human Resources Information Security Standards (Appendix 6)
- Information Protection Policy (Appendix 7)
- Computer, Telephone and Desk Use Policy (Appendix 8)
- Remote Working Policy (Appendix 9)
- Removable Media Policy (Appendix 10)
- Information Security Incident Management Policy (Appendix 11)
- IT Infrastructure Policy (Appendix 12)
- Data Protection
- Business Continuity
- Disposal and Destruction of Data
- Instant Messaging

A summary of the above as they apply to all users is included below, although employees should always refer to the relevant appendix for more detailed policy information.

5.1 Document Classification and Protective Marking Policy (Appendix 1)

Many organisations have formal documentation classification schemes. We have a responsibility to ensure we are aware of the data handling guidelines in relation to these documents or data. For these purposes documents are either paper whereas data is held in a business system database or as a raw data extract on Council filing systems. Electronic documents would usually be created using part of the Microsoft Office suite or in 'pdf' format but other forms may also exist. If in doubt always seek clarification from the data owner or your line manager.

The Government adopted a new classification scheme in 2014 and the Council has adopted this scheme. We should not receive any material classified as SECRET or TOP SECRET, any material classified as thus should be immediately deleted and the sender

notified. There are two classifications that will apply to each organisation: OFFICIAL and OFFICIAL SENSITIVE:

- OFFICIAL-SENSITIVE Broadly this includes data or documents that contain personal or personal sensitive data as defined by the Data Protection Act or defined under 'Special categories' under the General Data Protection Regulations. This can also include items that would be considered exempt under the Freedom of Information Act in relation to commercial sensitivity.
- OFFICIAL Covers all other documents and data that do not fall under the OFFICIAL-SENSITIVE classification and will form the majority of the Council data and documents

A full definition of the Government Classification Scheme can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

Key points to note:

- New documents which contain personal sensitive data as defined by the Data Protection Act or fall within a 'Special Category' under the General Data Protection Regulations should be protectively marked as OFFICIAL-SENSITIVE on both the header and footer of each page
- Amended documents should be protectively marked where not already marked
- Transmission of OFFICIAL-SENSITIVE material should be clearly marked as thus and appropriate steps taken to ensure transmission is secure
- Care should be taken with unmarked documents

Under the Data protection Act the following are defined as personal sensitive data:

- the racial or ethnic origin of the data subject,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- physical or mental health or condition,
- sexual life,
- the commission or alleged commission of any offence, or
- any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Under the General Data Protection Regulations in place from May 2018 the following are defined as 'Special Categories' of data or are covered elsewhere in the Regulation:

- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership

- Genetic data
- Biometric data
- Sex life or sexual orientation
- Physical and mental health
- Financial personal data
- Alleged criminal activity
- Criminal record

5.2 Email (Appendix 1)

- The use of email facilities will be permitted only by users that have been specifically designated as authorised users, received appropriate training and have confirmed in writing they accept and agree to abide by the terms of this policy.
- All emails that contain OFFICIAL-SENSITIVE information should be encrypted in transit when sent to other organisations whether in the public sector or not, see secure email guidance available on the Joint ICT Service intranet. Please contact the Joint ICT Service Desk if you are unsure if the recipient can receive secure email.
- Where correspondence is made directly with members of the public that contains OFFICIAL-SENSITIVE information it is not possible to ensure emails can be encrypted but all precautions to ensure the email address belongs to the intended recipient should be made.
- All correspondence which contains OFFICIAL-SENSITIVE material should be marked as such in the email title.
- Non-work email accounts **must not** be used to conduct or support official business.
- Users must ensure that any emails containing sensitive information must be sent from an official council email and be protected accordingly.
- All official external e-mail must carry the official council disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the equality legislation.
- Email should not be forwarded to personal email accounts under any circumstances.
- Auto forwarding of email to email addresses outside of the Council is not permitted.
- The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official the Council business should be considered to be an official communication from the council.
- The Council maintain their legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. The Council reserve the right, with written approval from an appropriate Director, Head of Service or the Human Resources Manager, to monitor emails sent within the Council email system…. without further notifying the individual concerned that the right is being exercised. Please see Appendix 1, specifically section 3.1, for further clarification on this issue.
- Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council ICT systems.

- It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

5.3 Internet Acceptable Usage (Appendix 2)

- Internet use is monitored by the Council.
- Users must familiarise themselves with the detail, essence and spirit of this policy before using the Internet facility provided.
- At the discretion of line manager, and provided it does not interfere with your work, the Council permits personal use of the Internet in your own time (for example during your lunch-break).
- Users are responsible for ensuring the security of their Internet account logon-id and password. Individual user log-on id and passwords should only be used by that individual user, and they should be the only person who accesses their Internet account.
- Users **must not** create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Users must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Any excess or 'out of tariff' charges incurred on Council provided broadband or mobile data contracts as a result of personal use must be reimbursed to the council in full.

5.4 Software (Appendix 3)

- All software acquired must be approved by the ICT Manager of the Joint ICT Service or their deputy.
- Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
- Every piece of software is required to have a licence and the Council will not condone the use of software that does not have a licence.
- Unauthorised changes to software **must not** be made.
- Users are not permitted to bring software from home (or any other external source) and load it onto Council computers.
- Users **must not** attempt to disable or reconfigure the personal firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

5.5 ICT Access (Appendix 4)

- All users must use strong passwords, see appendix 4 for details.
- Passwords must be protected at all times and must be changed at least every 60 days.
- It is a user responsibility to prevent their user ID and password being used to gain unauthorised access to the Council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the Council network without permission from the ICT Manager.
- Partners or 3rd party suppliers must contact the Joint ICT Service before connecting to the Council network.

5.6 Human Resources Information Security Standards (Appendix 5)

- All employees are expected to adhere to this policy
- Access to Information systems must be relevant to the jobholders role and duties
- All mandatory ICT training should be completed in a timely manner or access to systems will be removed
- In addition to normal recruitment verification checks carried out on all new employees' additional checks may be required, primarily when accessing systems and data provided by 3rd parties.

5.7 Information Protection Policy (Appendix 6)

- The Council must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the Government Security Classification scheme.
- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until their Line Manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- OFFICIAL-SENSITIVE information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing OFFICIAL-SENSITIVE classified information to any external organisation is also prohibited, unless via secure email.
- The disclosure of OFFICIAL-SENSITIVE information other than for approved purposes is a potential breach of the Data Protection Act and should be reported to the internal Data protection team.

5.8 Computer, Telephone and Desk Use (Appendix 7)

- Users must adhere to Council Telephone and Desk Use Policy at all times.
- Users should aim to maintain a clear desk at all times.
- the Council OFFICIAL-SENSITIVE information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.

5.9 Remote Working (Appendix 8)

- It is the users' responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention. Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- All OFFICIAL-SENSITIVE data held on portable computer devices must be encrypted.

5.10 Removable Media (Appendix 9)

- The use of all removable media devices such as USB memory sticks, data cards and writeable CD's and DVDs is prohibited unless a business case is agreed, training given, and agreement signed to this effect.
- Any removable media device that has not been supplied by IT **must not** be used.
- All data stored on removable media devices **must** be encrypted where possible, and personal data must not be stored on devices that are not encrypted. Only data that is authorised and necessary to be transferred should be saved on to the removable media device. N.B. Data that has been deleted can still be retrieved.
- Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.
- Damaged or faulty removable media devices must not be used.
- Special care **must** be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be taken to the IT section for secure disposal.
- Users should be aware of their responsibilities in regard to the Data Protection Act and General Data Protection Regulations and report any suspected breaches.

5.11 Information Security Incident Management (Appendix 10)

- All users should report any incidents or suspected incidents immediately by contacting the Joint ICT Service.
- Anonymity when reporting an incident can be maintained if desired.
- If an incident requires information to be collected for an investigation, strict rules must be adhered to. The Data Protection team should be contacted for guidance.
- Users should be aware of their responsibilities in regard to the Data Protection Act and report any suspected breaches.

5.12 ICT Infrastructure Security (Appendix 11)

- OFFICIAL-SENSITIVE information, and equipment used to store and process this information, must be **stored** securely.
- Desktop PCs should not have data stored on the local hard drive. This may require training and support from ICT for some users to migrate their files to network drives.
- Non-electronic information must be assigned an owner and a classification. OFFICIAL-SENSITIVE information must have appropriate information security controls in place to protect it.
- Users should be aware of their responsibilities in regard to the Data Protection Act and report any suspected breaches.
- Desktop PCs should not have data stored on the local hard drive.
- Equipment that is to be reused or disposed of must be returned to ICT to have all of its **data and software erased / destroyed**.

5.13 Data Protection

- All employees are expected to adherence to the Council's Data Protection practices and the specific policies listed supports compliance with the Data Protection Act 1998 and reduces the risk of data protection breaches.
- Full details and guidance are available on the Data Protection pages on the Council intranets.

5.14 Business Continuity

Electronic information assets are protected to ensure the Council business can continue in the event of significant physical disruption to one or more of the main Council sites. This includes:

- Physical security, arms and fire suppressant at main data centres
- Daily replication of data to designated disaster recovery sites for data managed by the Joint ICT Service
- Daily backups of data held offsite for data managed by the joint ICT Service. This data is retained for 30 days
- Corporate business continuity plans

5.15 Disposal and Destruction of Data

- Confidential waste bins are provided for the secure destruction of paper based records
- All unused electronic devices should be returned to the Joint ICT Service when no longer in use.
- All Council electronic data devices and removable are disposed of by the Joint ICT Service in accordance with regulation and for removable media and hard disks are destroyed to DOD 5220-22M standard
- Please refer to the Council Corporate Retention & Disposal Schedules

5.16 Instant messaging

- Some business applications now include the facility for 'Instant Messaging' (IM) between other users of the system.
- Any communications made by IM should be for business purposes only.
- The Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of IM by authorised users to ensure adherence to this Policy. The Council and Rykneld Homes Ltd reserve the right, with written approval from an appropriate Head of Service, to monitor IM sent within the Council business systems without further notifying the individual concerned that the right is being exercised.

6 Responsibility for Implementation

The following table identifies who within the Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Manager
Accountable	Section 151 Officer
Consulted	Human Resources, Data Protection Officer, User Group, Corporate Leadership Team
Informed	All Derbyshire Dales employees and all users as defined in the scope

7 Policy Compliance

All users will be required to undertake an ICT Induction and sign a declaration confirming they have received the training and confirm they will abide by the ICT Policies. A copy of this form can be seen in Appendix 13.

If any user is found to have breached this, or any policy contained within the Appendices attached, they will be subject to the Council disciplinary procedure, as appropriate. If a criminal offence is considered to have been committed the Council will support any action to assist in the prosecution of the offender(s).

If you do not understand the implications of this, or any policy contained within the Appendices attached, or how they may apply to you, seek advice from your line manager.

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorised disclosure or viewing of confidential data or information belonging to the Council

- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of the Council to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the Information Security Manager or their department or service manager.

8 Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would cause significant damage to the Council reputation or ability to operate
- If complying with the policy would breach Health and Safety.
- If an emergency, within the context of the emergency plan, arises

In such cases, the user concerned must take the following action:

- Ensure that a Council manager is aware of the situation and the action to be taken.
- Ensure that the situation and the actions taken are recorded in as much detail as possible and reported to the ICT Service Desk.
- Ensure that the situation is reported to the Information Security Manager as soon as possible.

- Failure to take these steps may result in disciplinary action.

In addition, ICT maintains a list of known exceptions and non-conformities to the policy. This list contains:

- Known breaches that are in the process of being rectified
- Minor breaches that are not considered to be worth rectifying
- Any situations to which the policy is not considered applicable.

Derbyshire Dales District Council will take no disciplinary action in relation to known, authorised exceptions to the information security management system.

This policy will be included within the Council Internal Audit Programme, and compliance checks will take place to review the effectiveness of its implementation.

9 Glossary of terms

Public Services Network(PSN) - This is a secure wide area network (WAN) that allows access to Central Government systems, secure data transfer, secure email and accredited solutions provided by public sector organisations and accredited 3rd parties. At present this includes gcsx secure email, CIS(Benefits), TellUsOnce and Electoral Registration systems. The scope of the PSN network covers local authorities, central government departments, National Health Service, the Criminal Justice Extranet and the Police National Network.

Government Security Classifications – a marking scheme of information assets as used by the UK Government. A new marking classification comes into effect from April 2nd 2014. Details of this scheme can be found via https://www.gov.uk/government/publications/government-security-classifications and the new marking classification guidelines can be found in Appendix A.

10 Contact Information

At the time of publication of this policy

the ***ICT Servicedesk*** is available on :-

- Self Service portal > http://sworksrv.ne-derbyshire.gov.uk/sw/selfservice/
- Email :- servicedesk@ne-derbyshire.gov.uk
- Telephone :- **3001** or 01246 21**7103**

- Monday to Friday 08:00am – 5:30pm

For incidents outside of these hours please contact the Information Security Manager who is the IT Manager.

APPENDIX 1 - E-MAIL POLICY

1. Introduction

Derbyshire Dales District Council will ensure all users of council email facilities are aware of the acceptable use of such facilities.

The Policy establishes a framework within which users of the Council's email facilities can apply self-regulation to their use of email as a communication and recording tool.

2. Scope

This policy covers all email systems and facilities that are provided by the Council for the purpose of conducting and supporting official business activity through the, The Council's network infrastructure and all stand alone and portable computer devices.

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees and individuals working on behalf of the Council, contractual third parties and agents, work experience and volunteers, who have been designated as authorised users of email facilities.

The use of email facilities will be permitted only by users that have been specifically designated as authorised users for that purpose, received appropriate training and have confirmed in writing that they accept and agree to abide by the terms of this policy.

The use of email facilities by users that have not been authorised for that purpose will be regarded as a disciplinary offence.

The policies are based on industry good practice and intend to satisfy the requirements set out by the Public Service Network Code of Connection.

References to protective marking schemes and guidance on assessing and handling such information are covered in Section 5.1 of the Information Security Policy

3. Email Policy

3.1 Email as Records

- All emails that are used to conduct or support the Council business must be sent using a "@<council>.gov.uk" address.
- Non-work email accounts **must not** be used to conduct or support official business.
- Users must ensure that any emails containing sensitive information must be sent from an official council email and be protected accordingly.
- All official external e-mail must carry the official council disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with equality legislation.
- For OFFICIAL-SENSITIVE information encryption **should** be used for all content and/or attachments that contain that classification. Secure email guidance is

available on the Joint ICT Service Intranet.

- Where secure email is **not** available to connect the sender and receiver of the email message, and information classified as OFFICIAL-SENSITIVE is being transferred, alternative encryption methods **must** be used for all content and/or attachments that contain that classification. The ICT Service Desk will advise on options available.
- Emails carrying OFFICIAL-SENSITIVE contents and/or attachments must be labelled to highlight the sensitivity and value that the information has to the data owner. This will be in the format of the Subject Header containing the label "OFFICIAL-SENSITIVE" as appropriate.
- Auto forwarding of email to email addresses outside of the Council is not permitted.
- Automatic forwarding of email within the organisations email system must be considered carefully to prevent OFFICIAL-SENSITIVE material being forwarded inappropriately.
- When handling data and documents provided by a 3rd party any document handling guidance provided by the 3rd party should be observed.

Non-work email accounts **must not** be used to conduct or support official Derbyshire Dales District Council business. Users must ensure that any emails containing sensitive information must be sent from an official council email. Any Council emails containing OFFICIAL-SENSITIVE information must be sent via secure email. All emails that represent aspects of Council business or Council administrative arrangements are the property of Council and not of any individual employee.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of user's activities.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Council business should be considered to be an official communication from the Council. In order to ensure that Council is protected adequately from misuse of e-mail, the following controls will be exercised:

i. It is a condition of acceptance of this policy that users comply with the instructions given during the email training sessions.
ii. All official external e-mail must carry the following disclaimer:

> *"Disclaimer*
>
> *This email is confidential, may be legally privileged and contain personal views that are not the views of* ***Derbyshire Dales District Council.***
>
> *It is intended solely for the addressee. If this email was sent in error please notify the sender, delete the email and do not disclose, copy, distribute, or rely on it. Under the Data Protection Act 1998 and the*

Freedom of Information Act 2000 the contents of this email may be disclosed.

This message and attached files have been virus scanned. Attachments are opened at your own risk."

Whilst respecting the privacy of authorised users, the Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Derbyshire Dales District Council reserves the right, with written approval from an appropriate Director, Head of Service or the Human Resources Manager, to monitor emails sent within the Council email system (including personal emails) and to access mailboxes and private directories without further notifying the individual concerned that the right is being exercised.

The Council may exercise this right, with approval from an appropriate Director, Hed of Service or Human Resources Manager and in accordance with the Data Protection Policy, in order to establish facts relevant to the Council business and to comply with:

- regulatory practices or procedures,
- to prevent or detect crime,
- to ensure compliance with Derbyshire Dales District Council policies,
- to investigate or detect unauthorised uses of the system or to ensure the effective operation of the system (e.g. to check if viruses are being transmitted).
- to ensure critical work or urgent items can be actioned.
- disclosure under the Data Protection Act 1998 or the Freedom of Information Act 2000.

In these circumstances you do not have a right to privacy when using the Council information systems or in relation to any communication generated, received or stored on the Council information systems.

These actions will be supervised by the Information Security Manager.

Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council ICT systems.

It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000. Further information regarding this can be obtained from the appropriate Data Protection Officer.

3.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most

appropriate method for conveying time critical or OFFICIAL-SENSITIVE information or of communicating in the particular circumstances.

All emails sent to conduct or support official Council business must comply with corporate communications standards. Council Communications and Operation Management Policy must be applied to email communications.

Email must not be considered to be any less formal than memo's or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council reputation or its relationship with customers, clients or business partners.

When sending emails internally or externally the user should exercise due care in selecting the recipients to send the communication to. This is particularly important when sending personal and sensitive data.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council 's Equal Opportunities Policies, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any material, should consult their line manager prior to commencing any associated activity or process.

IT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of OFFICIAL-SENSITIVE material concerning the activities of the Council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste users effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, marital status, disability, political, religion or belief, maternity or paternity, civil partnership, gender reassignment or sexual orientation.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For the use of impolite terms or language, including offensive or condescending

terms.

- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council into disrepute.

3.3 Unsolicited Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that they delete such messages without reading them or opening any attachments or hyperlinks. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Council systems or facilities.

3.4 Mail Retention

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addresses is discouraged.

Email content is also bound by Council Data retention policy and is covered by both the Data Protection and Freedom of Information Acts and, from May 2018, the General Data Protection Regulations(GDPR) and must be managed accordingly.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox.

3.5 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that the Council :

- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.

- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised use.
- To respond to formal complaints

Monitoring of content will only be undertaken by users specifically authorised for that purpose. These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

a. Establishing the existence of facts relevant to the business, client, supplier and related matters.
b. Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
c. Preventing or detecting crime.
d. Investigating or detecting unauthorised use of email facilities.
e. Ensuring effective operation of email facilities.
f. Determining if communications are relevant to the business.
g. It should also be noted that email and attachments may need to be disclosed under the Data Protection Act 1998 or the Freedom of Information Act 2000.

Where a manager suspects that the email facilities are being abused by a user, they should contact the ICT Manager and HR. Designated staff in the Joint ICT Service can provide evidence and audit trails of access to systems. The Joint ICT Service will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for this information.

Access to another employee's email is strictly forbidden unless the employee has given their consent, or their email needs to be accessed by their line manager for specific work purposes whilst they are absent. If the latter is the case the Council may exercise this right, with approval from an appropriate Director, Head of Service or the Human Resources Manager. This must be absolutely necessary and has to be carried out with regard to the rights and freedoms of the employee. Managers must only open emails which are relevant.

3.6 Classification of Messages

The Council has adopted the Government protective marking scheme. However we may handle data on behalf of 3rd parties who, as data owners, have adopted different protective marking schemes and data handling guidance. Please refer to section 5. of the Information Security Policy for further information.

3.7 Secure email

Emails sent between:

Derbyshiredales.gov.uk,

ne-derbyshire.gov.uk and

addresses are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, Council OFFICIAL-SENSITIVE material must not be sent via email unless assured as secure.

Where secure email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating OFFICIAL-SENSITIVE material.

Where secure email is not available to connect to the receiver of the email message, and information classified as OFFICIAL-SENSITIVE is being transferred, encryption should be used for all content and/or attachments that contain that classification. Please contact the Service Desk if the you are unsure if the recipient can receive secure email.

Emails carrying OFFICIAL-SENSITIVE contents and/or attachments must be labelled to highlight the sensitivity and value that the information has to the data owner. This will be in the format of the Subject Header containing the label "OFFICIAL-SENSITIVE" (with appropriate descriptor) as appropriate.

Please refer to the secure email guidance available on the Joint ICT Service Intranet.

3.8 Confidentiality

All users are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data (customers and employees). If any user is unsure of whether they should pass on information, they should consult the relevant Data Protection Officer.

Users must make every effort to ensure that the confidentiality of email is appropriately maintained. Users should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such networks and the number of people to whom the messages can be freely circulated without the knowledge of the Council.

Care should be taken when addressing all emails, but particularly where they include OFFICIAL-SENSITIVE information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent OFFICIAL-SENSITIVE material being forwarded

inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require assistance with this, please contact the ICT Servicedesk in the first instance.

3.9 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. If any user has concerns about possible virus transmission, they must report the concern to the Joint ICT Service and under no circumstances forward emails and attachments or open links in an email if there is any cause for concern.

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access the Council facilities.
- Must not forward virus warnings other than to the ICT Servicedesk.
- Must report any suspected files to the ICT Servicedesk.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted. Users must therefore comply with the Software Policy.

APPENDIX 2 - INTERNET ACCEPTABLE USAGE POLICY

1. Introduction

Derbyshire Dales Derbyshire District Council provide many and diverse Information and Communications Technology ("ICT") services, tools and equipment to employees to be used in the course of their work, including computers, laptops, telephones, internet and email.

The internet has become a fundamental tool which the Council use for research and education purposes. Internally, the Council have also developed an Intranet to aid the dissemination of relevant information amongst employees.

The Council support information and communications resources which will enhance the business and service environment. However, with access to computers and people all over the world via ICT comes the availability of material that may not be considered of value in the context of the Council setting. Additionally, as with any resource, there is the possibility of misuse. Accordingly, the Council need to set guidelines for the use of ICT and, where appropriate, to monitor its use.

However, even with the guidelines, the Council cannot prevent the possibility that some users may access material, even inadvertently, that is not consistent with the policies of the Council or in line with the normal duties and responsibilities of the user.

2. Scope

All information, whether electronic or paper based, relating to our customers, suppliers and business operations should be treated in line with (a) the Council Code of Conduct for Members and Officers, (b) relevant policies and (c) relevant legislation.

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees of the Council, contractual third parties and agents, work experience and volunteers who make use of the internet.

4. What is the Purpose of Providing the Internet Service?

4.1 General guidelines on use of the internet

Use of the Internet is available at your line manager's discretion. In general, users shall only use the Internet for official purposes, e.g. access to and the provision of information, research, electronic commerce. Use of information from the Internet shall be directly related to the official duties of the user, or the Council as a whole. All information downloaded from the Internet shall be related to the duties and tasks of the user. However, reasonable personal use is permitted within a user's own time at the discretion of their line manager.

Where there is public access to the Internet provided by the Council and a member of the public misuses this provision, it will not be deemed to be the responsibility of any

employee present at the time. However, the employee should report this incident as a breach of security to ICT.

Any information distributed or released by users by way of the Internet is subject to the Council guidance on the release of information and shall, prior to such distribution, be approved by the relevant management procedures.

Any proposed links from the Council Internet sites to the other Internet sites must first be authorised by a member of the senior management team.

Users must be aware that the quality and accuracy of information available on the Internet is variable. It is the responsibility of the individual user to judge whether the information obtained is satisfactory for the purpose for which it will be used, and, if appropriate, steps should be taken to verify this information independently.

Where the Internet is being accessed by employees via a mobile device (laptop or tablet, or smartphone) from an internet connection which is not covered by the Council internet filtering software, the same guidelines on appropriate use of the Internet apply and extra care must be taken not to visit sites which would be deemed unsuitable.

4.2 Specific Guidelines on Use of the Internet

- Software, including MP3 files, must not be downloaded from the Internet by users without the advice and permission of ICT personnel.
- When participating in newsgroups or mailing lists, users may offer information and advice to others if it is appropriate to their official duties or tasks or if the benefit to be gained by the Council represents a reasonable return in terms of the effort involved.
- Employees must not take part in discussions on political matters via the Internet unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited trade union representative.
- Users must not use their access to the Internet for their own private business purposes.
- Orders for goods purchased for the Council purposes must not be placed by way of the Internet without the employee having first obtained approval from their line manager, having authorised the purchase in the normal departmental manner and having complied with the council's Contract Standing Orders and Financial Regulations.
- Users must not use the Council Internet facility for the purpose of gambling.
- Users must not break or attempt to break any system security controls placed on their Internet Account.
- Users must not intentionally access or transmit computer viruses or software programs used to trigger these.
- Users must not intentionally access or transmit information which is obscene, sexually explicit, racist or defamatory or which depicts violent or criminal acts or otherwise represents values that are contrary to Council policy.
- Employees must not intentionally access or transmit information of a political nature unless this forms part of the legitimate business of their

employment or is in furtherance of their role as an accredited trade union representative.
- Users must not knowingly break the law.
- If an Internet site containing unsuitable material e.g. of an obscene nature is inadvertently accessed by a user, this must be immediately reported to ICT as a security breach.
- If material is inadvertently accessed which is believed to contain a computer virus, the user must immediately break the connection to the Internet and contact ICT for advice and assistance.
- Users must not copy information originating from others and re-post it without the permission of or acknowledgement to the original source.

5. Personal Use of the Internet Service

Any reasonable personal use of the Council ICT services and equipment must comply with the Council Code of Conduct for Officers and Members. Reasonable personal use of such services and equipment:-

- Must not be carried out in works time
- Must not interfere with the performance of your duties.
- Must not take priority over your work responsibilities
- Must not result in the Council incurring expense
- Must not have a negative impact on the Council.
- Must be lawful and in accordance with the Council Policy and with the guidelines as set out in this document.

Where reasonable personal use is referred to in this document, this section applies.

Reasonable personal use of the Council internet service is permitted only in the employee's own time (i.e. before clocking on, or after clocking off in accordance with the appropriate flexitime Scheme).

Any excess or 'out of tariff' charges incurred on Council provided broadband or mobile data contracts as a result of personal use must be reimbursed to the council in full.

6. Internet Account Management, Security and Monitoring

6.1 Monitoring and Reporting Internet Use

All access to the Internet is automatically logged against an identifier unique to the PC of the user, is recorded and may be monitored by the Council. This monitoring will be for the prevention and detection of unauthorised use of the Council communication systems.

Auditable statistics are kept within ICT of all Council Internet access.

Line managers are able to access details of sites visited by employees and the time spent accessing the internet. Such reporting is not provided on a set basis, but will be available to managers in the normal course of an investigation into inappropriate or prolonged use of the Internet by a user.

The Council ICT actively monitors access to inappropriate sites via the Internet security software. Any 'irregularities' encountered in this process are reported to the line manager of an employee in accordance with the Council Code of Conduct.

For Council, in the case of an investigation requiring to be carried out into the use of Internet access by a user, the relevant authority (this will be the line manager and/or Human Resources in the cases of an employee) will contact the Joint ICT Service who will access the necessary monitored information and provide a report of this to the relevant authority.

Internet filtering software is used to block access to sites which have been deemed unacceptable. In certain cases, where authorised by a line manager, users in specific posts may be allowed access to sites normally blocked to users where access to sites is required or helpful in the undertaking of the duties of the post.

The Council will provide a secure logon-id and password facility for your Internet account. The IT Section is responsible for the technical management of this account. You are responsible for the security provided by your Internet account logon-id and password. Only you should know your log-on id and password and you should be the only person who uses your Internet account.

7. Things You Must Not Do

Access to the following categories of websites is currently blocked using a URL filtering system:

- Adult/Sexual/Pornographic
- Alcohol and Tobacco
- Blogs, Forums and Web chat
- Drugs/Gambling
- Games/Downloads
- Hacking/Peer-to-peer
- Illegal/Criminal activity
- Religious extremism
- Offensive/Intolerance
- Hate and Discrimination
- Mobile Phones/Ringtones
- Personal Dating
- Some Search Engines
- Spyware/Spam URL's
- Violence and Weapons
- Suicide

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must **not** use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- Run a private business.
- Download any software that does not comply with the Council Software Policy.

The above list gives examples of "*unsuitable*" usage but is neither exclusive nor exhaustive. *"Unsuitable"* material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

In particular you are reminded that Powerpoint presentations with unsuitable images should not be downloaded.

8. Your Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use the Council Internet facility within the terms described herein.
- Read and abide by the following related policies:
    - Email Policy. (see Appendix 1)
    - Software Policy. (see Appendix 3)
    - IT Security Policy.(see Summary)

9. Whom Should I Ask if I Have Any Questions?

In the first instance you should refer questions about this policy to your Line Manager who will refer you to an appropriate contact. You should refer technical queries about the Council Internet service to the IT Manager.

APPENDIX 3 - SOFTWARE POLICY

1. Introduction

Derbyshire Dales District Council will ensure the acceptable use of software by all users of the Council computer equipment or information systems.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees of the Council, contractual third parties and agents, work experience and volunteers who make use of ICT equipment.

3. Software Policy

This policy sho**u**ld be applied at all times whenever using the Council computer equipment or Information systems.

3.1 Software Acquisition

All software acquired by the Council may only be purchased following consultation with the joint ICT service and approval provided by the ICT Manager or his deputy. Software may not be purchased through user corporate credit cards, petty cash, travel or entertainment budgets. Software acquisition channels are restricted to ensure that the Council has a complete record of all software that has been purchased and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers etc.) be loaded onto a Council machine as this may affect the performance of your device and the risk of introducing a virus.

4.2 Software Registration

The Council use software in all aspects of its business to support the work carried out by its employees. In all instances every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.

Software must be registered in the name of the Council, whichever is appropriate and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user.

The Joint ICT Service maintains a register of all software and will keep a library of software licenses. The register must contain:

a) The title and publisher of the software.
b) The date and source of the software acquisition.
c) The location of each installation as well as the serial number of the hardware on which each copy of the software is installed.
d) The existence and location of back-up copies.

e) The software product's serial number.
f) Details and duration of support arrangements for software upgrades.

Software on local area networks or multiple machines shall only be used in accordance with the licence agreement.

The Council holds licences for the use of a variety of software products on all Council Information Systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988, unless authorised by the software manufacturer.

It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

4.3 Software Installation

Software must only be installed by the Joint ICT Service once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by the Joint ICT Service.

Software may not be used unless approved by the ICT Manager, or their nominated representative.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software onto the Council systems without prior approval from Joint ICT Service

To maintain PSN compliance and to mitigate the risk of security vulnerabilities on version of software that are supported by the manufacturer of that software will be permitted. Where applicable a current support and maintenance agreement with the application provider should be in place.

4.4 Software Development

All software, systems and data development for the Council is to be used only for the purposes of the Council.

Software must not be changed or altered by any user unless there is a clear business need and approved by the ICT Manager of the Joint ICT Service. All changes to software should be authorised before the change is implemented. A full procedure should be in place and should include, but not be limited to, the following steps:

1. Change requests affecting a software asset should be approved by the software asset's owner.
2. All change requests should consider whether the change is likely to affect existing security arrangements and these should then be approved.
3. A record should be maintained of agreed authorisation levels.
4. A record should also be maintained of all changes made to software.

5. Changes to software that have to be made before the authorisation can be granted should be controlled.

4.6 Software Misuse

The Council will ensure that Firewalls and anti virus products are installed where appropriate. Users **must not** attempt to disable or reconfigure the Firewall or anti-virus software.

It is the responsibility of all Council users to report any known software misuse to the Joint ICT Service.

According to the Copyright, Designs and Patents Act 1988, illegal reproduction of software is subject to civil damages and criminal penalties. Any individual, who makes, acquires, or uses unauthorised copies of software will be disciplined as appropriate under the circumstances. Any illegal duplication of software may be treated as a disciplinary offence.

APPENDIX 4 - ICT ACCESS POLICY

1. Introduction

Access control r**u**les and procedures are required to regulate who can access Council information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Council or information in any format, and on any device.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Services, partners, employees of the Council, contractual third parties and agents, work experience and volunteers who access ICT services.

3. Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

4. Applying the Policy - Passwords

4.1 Choosing passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and strong passwords

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words that may be present in a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Strong passwords should be used with a minimum standard of:

- At least eight characters.
- Contain a mix of alpha and numeric, with at least one digit
- Contain a mix of upper and lower case with at least one upper case character

4.2 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your user name within the password.
- Do not use the same password for systems inside and outside of work.

4.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 60 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the Joint ICT Service.

Users **must not** reuse the same password within 20 password changes.

5. System Administration Standards

All Council IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users- i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

6. Applying the Policy – Employee Access

6.1 User Registration

A request for access to the council's computer systems must first be submitted to the Joint ICT Service for approval. Applications for access must only be submitted if approval has been gained from your line manager.

When a user leaves the Council, their access to computer systems and data must be suspended at the close of business on the user's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the Joint ICT Service and the relevant business system administrators.

6.2 User Responsibilities

It is a users responsibility to prevent their user ID and password being used to gain unauthorised access to the Council systems by:

- Following the password policy and statements outlined above.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the Joint ICT Service and the relevant business system administrators of any changes to their role and access requirements.

6.3 Network Access Control

Connecting non Council devices to the Council networks is strictly forbidden without prior approval and risk assessment by the Joint ICT Service.

7. Users Authentication for External Connections

Where remote access to the Council network is required, an application must be made to the Joint ICT Service. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a biometric device or authentication token. For further information please refer to the Remote Working Policy (Appendix 9).

7.1 Supplier's Remote Access to the Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council network without permission from the Joint ICT Service. Any changes to supplier's connections must be immediately sent to the Joint ICT Service so that access can be updated or ceased. All permissions and access methods must be controlled by the Joint ICT Service.

Partners or 3rd party suppliers must contact the Joint ICT Service before connecting to the Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

APPENDIX 5 - HUMAN RESOURCES INFORMATION SECURITY STANDARDS POLICY

1. Introduction

Derbyshire Dales Derbyshire District Council holds large amounts of personal and protectively marked information. Information security is very important to help protect the interests and confidentiality of the Council and their customers. Information security cannot be achieved by technical means alone. Information security must also be enforced and applied by people, and this policy addresses security issues related to people.

2. Scope

This policy applies to all users that require access to the Council information systems or information of any type or format (paper or electronic).

The definition of users within this policy is intended to include all Services, partners, employees of the Council, contractual third parties and agents, work experience and volunteers who have access to ICT equipment

Where access is to be granted to any third party (e.g. contractors, service providers, voluntary agencies, partners) compliance with this policy must be agreed and documented. Responsibility for ensuring this lies with the Council user that initiates this third party access.

3. Principles

The Council understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to the Council information systems **must**:

- Be suitable for their roles.
- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information relevant to the jobholders role and duties.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after any users access to information or information systems used to deliver the Council business.

Access to the Council information systems will not be permitted until the requirements of this policy have been met.

4. Roles and Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the Information Asset Owner – please refer to Information Protection Policy (see Appendix 7).

Line managers are responsible for ensuring that creation of new users, changes in role, and termination of users are notified to the Joint ICT Service in a timely manner, using an agreed process.

The information security responsibilities of every user include familiarisation with the Information Security Policy and its Appendices, and the signing of a statement confirming that the user is aware of, and understands, these policies. (See Appendix 13)

4.1 User Screening

Background verification checks are carried out on all employees by HR, please see the HR recruitment and selection policy for details.

ICT staff with network administration rights and, where appropriate or required by 3rd party agreements, will also require standard checks through the Disclosure and Barring Service.

Where access is to systems processing payment card data, credit checks on the user must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

4.2 Management Responsibilities

Line managers must notify ICT in a timely manner of any changes in a users role or business environment, to ensure that the user access can be changed as appropriate.

Processes must ensure that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

Any changes to a users access must be made in a timely manner and be clearly communicated to the user.

Service managers must require users to understand and be aware of information security threats and their responsibilities in applying appropriate Council policies. These policies include:

- Information Protection Policy (Appendix 7)
- Information Security Incident Management Policy (Appendix 11)

This requirement must be documented.

4.3 Information Security Awareness, Education and Training

All users of ICT systems are required to undertake n security awareness training and should take note of updates in related statute and organisational policies and procedures as relevant for their role.

It is the role of Service managers to ensure that their users are adequately trained and equipped to carry out their role efficiently and securely.

5. Applying the Policy – When Access to Information or Information Systems is No Longer Required

5.1 Secure Termination of Employment

Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project. The key requirement is that access to Council information assets is removed in a timely manner when no longer required by the user

5.2 Return of Assets

Users must return all of the organisation's assets, for example, laptops, tablets, mobile phones, memory sticks in their possession upon termination of their employment, contract or agreement. This must include any copies of information in any format.

APPENDIX 6 - INFORMATION PROTECTION POLICY

1. Introduction

Information is a major asset that Derbyshire Dales Derbyshire District Council has a responsibility and requirement to protect.
Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Council maintains. It also covers the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at the Council. The policy specifies the means of information handling and transfer within the Council.

2. Scope

The policy applies automatically to all the systems, people and business processes that make up the Council information systems.

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of the Council, contractual third parties and agents, work experience and volunteers who have access to Information systems or information used for the Council purposes.

3. Principles

The Council will ensure the protection of all information assets within the custody of the Council.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

This policy should be applied whenever the Council Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape, DVD or video.
- Speech.

4. Applying the Policy

4.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, mobile devices, removable media).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

The Council must draw up and maintain inventories of all important personal data assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

4.2 Data Retention

The Council have data retention policies in place.

4.3 Personal data

Personal data is any information about any living, identifiable individual. This could be customer, employee, or member personal data. The Council is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998. Details of specific requirements can be found in the Legal Responsibilities Policy.

4.4 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

4.5 Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done.

4.6 Information Assets with Short Term or Localised Use

For new documents that have a specific, short term localised use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by users. All users must be informed of their responsibility for the documents they create.

4.7 Corporate Information Assets

For information assets whose use throughout the Council is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

4.8 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

Users are not allowed to access information until a line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

Databases holding personal information have a defined security and system management procedure for the records and documentation.

This documentation will include a clear statement as to the use, or planned use of the personal information.

Files which are identified as a potential security risk should only be stored on secure network areas.

5. Disclosure of Information

5.1 Sharing OFFICIAL-SENSITIVE Information with other Organisations

OFFICIAL-SENSITIVE information **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Exchange Agreement.

An official email legal disclaimer must be contained with any email sent. This can be found in the Email Policy.

The disclosure of OFFICIAL-SENSITIVE information in any way other than via secure email is a disciplinary offence. If there is suspicion of a user treating OFFICIAL=SENSITIVE information in a way that could be harmful to the Council or to the data subject, then it is be reported to the internal audit section, and the person may be subject to disciplinary procedure.

Any sharing or transfer of the Council information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

APPENDIX 7 - COMPUTER, TELEPHONE AND DESK USE POLICY

1. Introduction

Modern day business operations and advances in technology have necessitated the wide spread use of computer facilities into most offices within Derbyshire Dales District Council and, with the advent of portable computers, away from the Council premises.

As such, there is considerable scope for the misuse of computer resources for fraudulent or illegal purposes, for the pursuance of personal interests or for amusement/entertainment. The Council also handle large amounts of OFFICIAL-SENSITIVE information. The security of this information is of paramount importance. Working towards a clear desk policy can help prevent the security of this information from being breached.

The purpose of this document is to establish guidelines as to what constitutes "computer and telephony resources", what is considered to be "misuse" and how users should work towards a clear desk environment.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of the Council, contractual third parties and agents, work experience and volunteers who have access to information systems or information used for Council purposes.

3. Principles

This policy should be applied whenever users who access information systems or information utilise Council computer and telephony resources.

Computer and telephony resources include, but are not restricted to, the following:

- Centralised server and storage systems
- Hosted solutions(Cloud)
- Personal computers.
- Portable laptop computers.
- Removable media (memory cards and sticks)
- Mobile devices(smart phones, tablets)
- Printers.
- Network equipment.
- Telecommunications facilities.

4. Computer Resources Misuse

No exhaustive list can be prepared defining all possible forms of misuse of computer resources. The individual circumstances of each case will need to be taken into account. However, some examples are outlined below:

- Use of computer resources for the purposes of fraud, theft or dishonesty.
- Storing/loading/executing of software for a purpose which is not work related.
- Storing/loading/executing of software:
    - which has not been acquired through approved Council procurement procedures, or
    - for which the Council does not hold a valid program licence, or
    - which has not been the subject of formal virus checking procedures.
- Storing/processing/printing of data for a purpose which is not work related.

For further information, users are requested particularly to read the following policies:

- Email Policy (Appendix 1)
- Internet Acceptable Use Policy (Appendix 2)
- Software Policy (Appendix 3)

5. Clear Desk

The Council has a Clear Desk Policy which is available via the intranet which is to ensure to ensure that all information is held securely at all times

Documents should not be left lying on printers, photocopiers or fax machines.

Users of IT facilities are responsible for safeguarding data by ensuring that equipment is not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

Computer screens must be locked to prevent unauthorised access when unattended and screens should lock automatically after a 10 minute period of inactivity, in order to protect information. A screen saver with password protection enabled must be used on all PCs. Attempts to tamper with this security feature will be investigated and could lead to disciplinary action. The screen saver should be the one supplied by IT, no personal screen savers are to be used.

Users of hot desk stations must ensure that it is left in the state in which it was found.

Remember, when you are not working at your workstation there could be a business requirement for other users to use that station.

APPENDIX 8 - REMOTE WORKING

1. Introduction

Derbyshire Dales Derbyshire District Council provides portable computing devices to assist users to conduct official Council business efficiently and effectively. This equipment, and any information stored on portable computing devices, should be recognised as valuable organisational information assets and safeguarded appropriately.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of the Council, contractual third parties and agents, work experience and volunteers who use Council IT facilities and equipment when working on official business away from the organisation (i.e. working remotely), or who require remote access to Council information Systems or information.

3. Principles

Council information systems or information must not be accessed whilst outside the United Kingdom regardless of who owns the IT equipment.

Portable computing devices include, but are not restricted to, the following:

- Laptop computers.
- Smartphones
- Tablets
- Tablet PCs.
- Mobile phones.
- Wireless technologies.

4. Applying the Policy

All IT equipment (including portable computer devices) purchased for users by the Council is the property of the purchaser. It must be returned upon the request of the purchaser. All IT equipment will be supplied and installed by Joint ICT Service staff. Hardware and software **must only** be provided by the purchasers.

Where users access Central Government IT systems including secure gcsx email, **under no circumstances** should non-Council owned equipment be used.

5. User Responsibility

It is the user's responsibility to ensure that the following points are adhered to at all times:

- Users must take due care and attention of portable computer devices when moving between home and another business site.
- Users will not install or update any software on to a Council owned portable computer device.

- Users will not install any screen savers on to a Council owned portable computer device.
- Users will not change the configuration of any Council owned portable computer device.
- Users will not install any hardware to or inside any Council owned portable computer device, unless authorised by the Joint ICT service.
- Users will allow the installation and maintenance of Council installed Anti Virus updates immediately.
- Users will inform the Joint ICT Service of any Council owned portable computer device message relating to configuration changes.
- Business data should be stored on a Council file and print server wherever possible and not held permanently on the portable computer device
- All faults must be reported to the Joint ICT Service.
- Users must not remove or deface any asset registration number.
- Users registration must be requested from the Joint ICT Service. Users must state which applications they require access to.
- Users requests for upgrades of hardware or software must be approved by a line manager. Equipment and software will then be purchased and installed by ICT Services.
- The IT equipment can be used for personal use by users so long as it is not used in relation to an external business and does not conflict with Council business or policies. Only software supplied and approved by the ICT Service. can be used (e.g. Word, Excel, Adobe, etc.).
- No family members may use the ICT equipment. The ICT equipment is supplied for the users sole use.
- The user must ensure that reasonable care is taken of the IT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, Council may recover the costs of repair.
- The user must not take any Council supplied ICT equipment outside the United Kingdom as the equipment may not be covered by the Council normal insurance against loss or theft and it is liable to be confiscated by airport security personnel.
- The Council may at any time, and without notice, request software and hardware audits, and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit.
- Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database, or carry out any processing of OFFICIAL-SENSITIVE information relating to the Council, its employees, or customers. **Under no circumstances** should personal or security marked information be emailed to a private non-Council email address. For further information, please refer to the Email Policy.
- Any data transferred from Council systems must only be undertaken using a Council provided encrypted memory stick.
- Any users accessing PSN services or facilities, or using OFFICIAL-SENSITIVE information, must only use Council owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely.
- Users should not leave computer devices in unattended vehicles.
- Any loss of equipment should be reported immediately to the ICT Service Desk and, if appropriate, to the Data Protection Officer.

6. Remote and Mobile Working Arrangements

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should also be located out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. Equipment must be secured whenever it is not in use

No removable media devices or paper documentation should be stored with the portable computer device.

Paper documents are vulnerable to theft if left accessible to unauthorised people, and the onus is on the employee to maintain confidentiality. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. All documents classified as OFFICIAL-SENSITIVE must be disposed of via confidential waste facilities.

7. Access Controls

It is essential that access to all OFFICIAL-SENSITIVE information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or user login controls.

Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on portable computer devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL-SENSITIVE data held on the portable device must be encrypted. Personal data can only be stored on encrypted devices. It is ICTs responsibility to provide encrypted devices and the employees to ensure they are used.

Only methods approved and provided by the Joint ICT Service must be configured to allow remote access to the Council systems if connecting over Public Networks, such as the Internet.

Dual-factor authentication must be used when accessing the council network and information systems (including Outlook Web Access) remotely via both the Council owned and non-council owned equipment

Access to the Internet from Council owned ICT equipment, should only be allowed via onward connection to the Council provided proxy servers and not directly to the Internet. It is the employees responsibility to ensure this.

8. Anti Virus Protection

All Council devices have anti virus protection. Under no circumstances should this be disabled or modified.

9. Users Awareness

All users must comply with appropriate codes and policies associated with the use of IT equipment as contained within the Information Security Policy and its appendices.

All users must have attended mandatory Security Awareness Training and Data Protection training.

It is the user's responsibility to ensure their awareness of and compliance with these.

The user shall ensure that appropriate security measures are taken to stop unauthorized access to OFFICIAL-SENSITIVE information, either on the portable computer device or in printed format. Users are bound by the same requirements on confidentiality and Data Protection as the Council are.

APPENDIX 9 - REMOVABLE MEDIA POLICY

1. Introduction

This policy establishes the principles and working practices that are to be adopted by all users in order for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of the Council . computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.
- Maintain high standards of care in ensuring the security of Protected and Restricted information.
- Prohibit the disclosure of information as may be necessary by law.

A definition of the national protective marking scheme and government security classifications can be found in the PSN acceptable usage policy (see appendix 5).

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Derbyshire Dales Derbyshire District Council, contractual third parties and agents, work experience and volunteers who have access to Council information systems or IT equipment and intends to store any information on removable media devices.

3. Principles

The Council will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

Removable media devices include, but are not restricted to the following

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.

- Audio Tapes (including Dictaphones and Answering Machines)
- Video tapes

4. Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. Information is used throughout the Council and sometimes shared with external organisations and applicants. Securing OFFICIAL-SENSITIVE data is of paramount importance – particularly in relation to the council's need to protect data in line with the requirements of the Data Protection Act 1998 Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the Council. It is therefore essential for the continued operation of the Council that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the Council needs.

5. Restricted Access to Removable Media

It is the Council policy to prohibit the use of all removable media devices without approval. The use of removable media devices will only be approved if a valid business case for its use is developed. There are significant risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made to the IT Section. Approval for their use must be given by a Service Manager, this should be done via a request to the service desk. This applies to the devices themselves, including memory sticks but not the media such as CD's, DVD's and audio and video tapes.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

6. Procurement of Removable Media

All removable media devices, including memory sticks, and any associated equipment and software must only be purchased and installed by ICT Services. Procurement of consumable media such as CD's, DVD's and audio and visual may be procured through standard procurement channels. Non-council owned removable media devices and media **must not** be used to store any information used to conduct official Council business, and **must not** be used with any Council owned or leased IT equipment.

The only equipment and media that should be used to connect to Council equipment or the Council network is equipment and media that has been purchased by the Council and approved by the Joint ICT Service or has been sanctioned for use by the IT Manager.

7. Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data which is frequently backed up. Therefore removable media should not be the only place where data obtained for the Council purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system. For further information please see the Remote Working Policy (see Appendix 9).

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted. If this is not possible, then all OFFICIAL-SENSITIVE data or personal or sensitive data held must be encrypted.

Users should be aware that the Council will audit / log the transfer of data files to and from all removable media devices and Council owned IT equipment.

8. Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to the Joint ICT Service who will access the breach to determine the appropriate course of action. The Data Protection Officer should also be informed where appropriate.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the ICT Manager as referenced in the Information Security Incident Management Policy (see Appendix 11).

9. Third Party Access to Council Information

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the Council network, information stores or IT equipment without explicit agreement from the Joint ICT Service ICT Manager and the Data Protection Officer.

Should third parties be allowed access to the Council information then all the considerations of this policy apply to their storing and transferring of the data.

10. Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the Joint ICT Service should removable media be damaged and return to ICT for secure disposal.

Virus and malware checking software approved by the Joint ICT Service must be operational on any device managed and owned by the Council. It is the users responsibility to ensure appropriate and up to date virus and malware software is operational on any non Council device that the removable media device is connected to or seek assurances to that effect.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage.

11. Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused, either within the Council or for personal use, must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. **All removable media devices that are no longer required, or have become damaged, must be returned to the Joint ICT Service for secure disposal**.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the Joint ICT Service.

12. Users Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices.

APPENDIX 10 - INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

1. Introduction

This policy needs to be applied as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

The definition of an "information management security incident" ('Information Security Incident' in the remainder of this policy and procedure) is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An information security incident includes, but is not restricted to, the following:

- The loss or theft or corruption of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all Departments, partners, employees of Derbyshire Dales Derbyshire District Council, contractual third parties and agents, work experience and volunteers who have access to Council information systems or IT equipment.

All users **must** understand and adopt use of this policy and are responsible for ensuring the safety and security of the Council systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Malicious

- Giving information to someone who should not have access to it - verbally, in writing or electronically.

- Computer infected by a Virus or other malware.

- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

Misuse

- Use of unapproved or unlicensed software on Council equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
- Sending a sensitive e-mail to 'all staff' by mistake
- Writing down your password and leaving it on display / somewhere easy to find.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / Loss

- Theft / loss of a hard copy file.
- Theft / loss of any Council computer equipment.

4. Procedure for Incident handling

Events and weaknesses need to be reported at the earliest possible stage as they need to be assessed by the Joint ICT Service in order to identify when a series of events or weaknesses have escalated to become an incident. It is vital for the Joint ICT Service to gain as much information as possible from the business users to identify if an incident is occurring.

The following sections detail how users must report information security events or weaknesses.

4.1 Reporting Information Security Events for all Employees

Security events, for example a virus infection, could quickly spread and cause data loss across the organisation. All users must understand, and be able to identify that any unexpected or unusual behaviour on the workstation could potentially be a software malfunction. If an event is detected users **must**:

- Note the symptoms and any error messages on screen.
- Disconnect the workstation from the network if an infection is suspected (with assistance from ICT support staff.
- Not use any removable media (for example USB memory sticks) that may also have been infected.

All suspected security events should be reported immediately to the ICT Service Desk on ext 3001 or external number 01246 217103.

If the Information Security event is in relation to paper or hard copy information, for example personal information files that may have been stolen from a filing cabinet, this must be reported immediately to senior management and the Data Protection Officer for the impact to be assessed.

The Joint ICT Service will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident.
- The type of data, information or equipment involved.
- Whether the loss of the data puts any person or other data at risk.
- Location of the incident.
- Inventory numbers of any equipment affected.
- Date and time the security incident occurred.
- Location of data or equipment affected.
- Type and circumstances of the incident.

The Data Protection Officer will require:

- A contact name and number of the person reporting the incident
- Type of data
- Details of steps already taken

4.2 Reporting Information Security Weaknesses for all Employees

Security weaknesses, for example a software malfunction, must be reported through the same process as security events. Users must not attempt to prove a security weakness as such an action may be considered to be misuse.

Weaknesses reported to application and service providers by employees must also be reported internally to the Joint ICT Service. The service provider's response must be monitored and the effectiveness of its action to repair the weakness must be recorded by the Joint ICT Service.

4.3 Collection of Evidence

If an incident may require information to be collected for an investigation strict rules must be adhered to. The collection of evidence for a potential investigation must be approached with care. Internal Audit must be contacted immediately for guidance and strict processes must be followed for the collection of forensic evidence. If in doubt

about a situation, for example concerning computer misuse, contact the Joint ICT Service for advice.

The actions required to recover from the security incident must be under formal control. Only identified and authorised users should have access to the affected systems during the incident and all of the remedial actions should be documented in as much detail as possible.

The officer responsible for an incident should risk assess the incident based on the Corporate Risk Impact Methodology.

APPENDIX 11 - IT INFRASTRUCTURE SECURITY POLICY

1. Introduction

The purpose of this policy is to establish standards in regard to the physical and environmental security of the Council information, in line with section A9 of ISO/IEC/27001.

In order to ensure the continued protection of the personal, confidential and protectively marked information (see Glossary) information that the Council holds and uses, and to comply with legislative requirements, information security best practice, and, newly mandated security frameworks such as those attending credit and debit card transactions and access to the Public Services Network(PSN), access to Council information equipment and information must be protected.

This protection may be as simple as a lock on a filing cabinet or as complex as the security systems in place to protect the Council IT data centre. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. No service should fall below the baseline security standard level of protection required for their teams and locations.

2. Scope

This policy applies to all users. The definition of users within this policy is intended to include all departments, partners, employees of the Council contractual third parties and agents, work experience and volunteers who have access to Council information equipment and information (electronic and paper records). They are responsible for ensuring the safety and security of the Council equipment and the information that they use or manipulate.

3. Principles

There shall be no unauthorised access to either physical or electronic information within the custody of the Council.

Protection shall be afforded to:

- IT equipment that hold Electronic data
- IT equipment used to access electronic data.
- IT equipment used to access the Council network.

This policy applies to all users of the Council owned or leased / hired facilities and equipment. The policy defines what paper and electronic information belonging to the Council should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution users make to the safe and secure use of information within the custody of the Council.

This policy should be applied whenever a user accesses the Council information equipment. This policy applies to all locations where information within the custody of the Council or information processing equipment is stored, including remote sites.

4. Secure Areas

OFFICIAL- SENSITIVE information **must** be stored securely. A risk assessment should identify the **appropriate** level of protection to be implemented to secure the information being stored.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours.
- Window and door locks.
- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g. fire, flood, vandalism.

Access to secure areas such as the data centre and ICT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons. Users working in secure areas should challenge anyone not wearing a staff or visitor badge. Each Service must ensure that doors and windows are properly secured at the end of each working day.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A

council ICT employee must monitor all visitors accessing secure ICT areas at all times.

Keys to all secure areas housing ICT equipment and lockable ICT cabinets are held centrally by the ICT Service, as appropriate. Keys are not stored near these secure areas or lockable cabinets.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach.

If a user leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the users and any door/access codes should be changed immediately. Please also refer to the ICT Access Policy and Human Resources Information Security Standards.

6. Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g. **if necessary** items such as laptops should be physically attached to the desk.
- If laptops or tablets must be left at the office overnight then they should be kept out of sight, preferably in a locked drawer or cabinet
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs and laptops should not have data stored on the local hard drive. Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from ICT Services.

All items of equipment must be recorded on an inventory, maintained by ICT. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of.

All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the ICT inventory.

For portable computer devices please refer to the Remote Working Policy (appendix 9).

7. Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas, Health and Safety guidance should be sought if in any doubt.

8. Security of Equipment off Premises

Please refer to the Remote Working Policy.

9. Secure Disposal or Re-use of Equipment

Equipment that is to be reused or disposed of must be returned to the Joint ICT Service for data removal.

Software media or services must be returned to ICT to be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

BACK TO AGENDA

NOT CONFIDENTIAL – For public release Item No. 12

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Resources

ICT PROJECTS FOR CAPITAL PROGRAMME 2017-19

PURPOSE OF REPORT

To seek for additional capital projects related to ICT in 2017/18 and 2018/19.

RECOMMENDATION

1. That Committee approve the business cases for:

    a. Virtual Desktop Server replacement
    b. Microsoft Windows Server license upgrade
    c. Income Management system upgrade

2. That, subject to the approval of recommendation 1, Council be requested to approve funding for these projects within the revised capital programme.

WARDS AFFECTED

None

STRATEGIC LINK

Adequate provision of ICT facilities will help to provide services efficiently and to reduce the risks of service disruption, supporting the achievement of all Council objectives.

---

1 SUMMARY

1.1 The joint ICT service, in conjunction with the Head of Resources, maintain a five year capital investment plan to ensure out ICT infrastructure is fit for purpose.

A number of these investment schemes are now ready to progress in the current financial year or early in 2018-19.

2. REPORT

2.1 Virtual Desktop Server Replacement – Estimated Capital Cost £28,000

In 2012 a new infrastructure solution was implemented at Derbyshire Dales to provide a ‘virtual desktop’ solution. There were three key reasons for this solution:

1) To provide flexible working arrangements for staff;

2) To facilitate the external use of Derbyshire Dales systems by Arvato (who provide the Council's Revenues and Benefits service, mainly from Chesterfield);
3) To provide a cost effective means for the deployment of Windows 7 across the organisation.

The server infrastructure is now 5 years old and is therefore due for replacement as part of the agreed refresh lifecycle for ICT infrastructure. In addition, the existing server infrastructure will not have sufficient capacity to run virtual desktops running Windows 10. Windows 10 is the next Windows desktop operating system, which the Council must migrate to before January 2020 when extended security support from Microsoft will end.

As part of our Public Service Network (PSN) compliance The Council is required to maintain fully supported operating systems. The replacement server will meet this need and will also minimise the risks of business disruption.

The estimated capital cost of this project is £28,000, which is requested for the financial year 2017/18.

2.2 Microsoft Windows Server license upgrade – Estimated Capital Cost £12,000

In 2012 Derbyshire Dales District Council invested in 'data centre' licences to allow our windows based server estate to be upgraded to Windows Server 2012.

Whilst Microsoft commit to providing security support for its products for 10 years, most business application vendors will only certify and support their products on two prior versions of the Windows Server products.

Since the release of Windows Server 2012 two new iterations of the product have been released, R012R2 and 2016. Roadmaps from some vendors indicate that support for Windows 2012 will be dropped during 2018.

At current prices, £12,000 will be required to fund this upgrade, which we would be looking to carry out in 2018/19.

2.3 Income Management system upgrade – Estimated Capital Cost £15,000

The Council's Income Management System has been used for many years to assist in accounting for income. Considerable investment has been made to tailor the system to meet the Council's business needs. The system has been updated in recent years to provide facilities for website payments and for an automated telephone payments facility.

The vendor, Capita Business Systems Limited, has indicated that the Council must upgrade to version 11 of the system in order to remain fully supported.

As part of our Public Service Network (PSN) compliance The Council is required to maintain fully supported operating systems. The upgraded system will meet this need and will also minimise the risks of business disruption.

The estimated capital cost of this project is £15,000, which is requested for the financial year 2017/18. This cost is based on a joint project with North East Derbyshire District Council and the price being accepted by 30 September 2017.

3 RISK ASSESSMENT

3.1 Legal

The procurement route, should finance be made available will be in accordance with Contract Standing Orders. The legal risk is therefore low.

3.2 Financial

It will be necessary to seek approval from Council for the investment in these projects. The total cost of these three projects is £55,000. The financial risk arising from this report is, therefore, assessed as high.

4 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

5 CONTACT INFORMATION

Karen Henriksen, Head of Resources
Telephone: 01629 761284; Email: karen.henriksen@derbyshiredales.gov.uk

Nick Blaney, ICT Manager
Telephone: 01246 217097; Email: nick.blaney@ne-derbyshire.gov.uk

6 BACKGROUND PAPERS

None

NOT CONFIDENTIAL – for public release **Item No.** 13

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Corporate Director

LAND HOLDINGS REVIEW

SUMMARY

This phase of the Land Holdings Review covers 2 sites across the District in which expressions of interest or requests to purchase a site or granting a lease have been received. Following detailed consideration of planning, legal and estate management factors, recommendations are made regarding whether the sites should be sold or lease confirmed and the terms which would apply.

RECOMMENDATION

1 That the interested party in respect of site 1 be informed that their request to purchase the freehold is accepted with terms as indicated in Appendix 1 of this report.

2 That a new lease is authorised in respect of site 2 as indicated in Appendix 1of this report.

WARDS AFFECTED

Wirksworth, Hathersage & Eyam,

STRATEGIC LINK

The Land Holdings Review Process accords with the District Council's values and aims of obtaining "value for money" and to "protect and enhance the environment" as outlined in the 2015-2019 Corporate Plan.

---

1 REPORT

1.1 Background

This phase of the Land Holdings Review covers 2 sites across the District in which expressions of interest or requests to purchase a site or grant a lease have been received. Following detailed consideration of planning, legal and estate management factors, recommendations are made regarding whether the sites should be sold or lease approved and the terms which would apply.

1.2 **Review Procedure**

An appraisal of each site has taken place comprising advice on any planning constraints, legal restrictions and maintenance liabilities plus an assessment of any health and safety risks.

The results and recommendations are summarised in Appendix 1 together with plans of each site.

1.3 Summary of Outcome

1 no. site is recommended for disposal
1 no. site is recommended for authorising the granting of a lease

1.4 Consultation

Where it is recommended that a site be sold, the relevant Local Council and Ward Members have been consulted and any responses received will be reported at the meeting.

1.5 Planning Consents

In each case of disposal the purchaser would be responsible for making any necessary planning application at their cost to enable their desired use of the site. The decision at this meeting is entirely without prejudice to any future decisions on such applications by this Council as Planning Authority.

2 RISK ASSESSMENT

2.1 **Legal**

The Council has a duty under S123 of the Local Government Act 1972 to dispose of assets for the best price reasonably obtainable.

The purchasers would be responsible for the District Council's reasonable legal costs.

The duty to consult on any disposals accords with the Council's policy on the disposal of land and property. The legal risk in that respect is low.

2.2 **Financial**

Site 1 : The Council has no financial interest to protect in the disposal of this site. The financial risk is assessed as 'low".

Site 2: The lease will provide the Council with annual income of £4,000pa which is similar to its potential earning as a Council car park. The lessor will pay the Council's legal fees. The financial risk is assessed as "low".

3 OTHER CONSIDERATIONS

In preparing this report the relevance of the following factors is also been considered: prevention of crime and disorder, equality of opportunity, environmental health, legal and human rights, financial personal and property considerations.

4 CONTACT INFORMATION

Mike Galsworthy, Estates and Facilities Manager
Tel: 01629 761207 E-mail: mike.galsworthy@derbyshiredales.gov.uk

5 BACKGROUND PAPERS

Property Services File – Land Holdings Review

Appendix 1

LAND HOLDINGS REVIEW

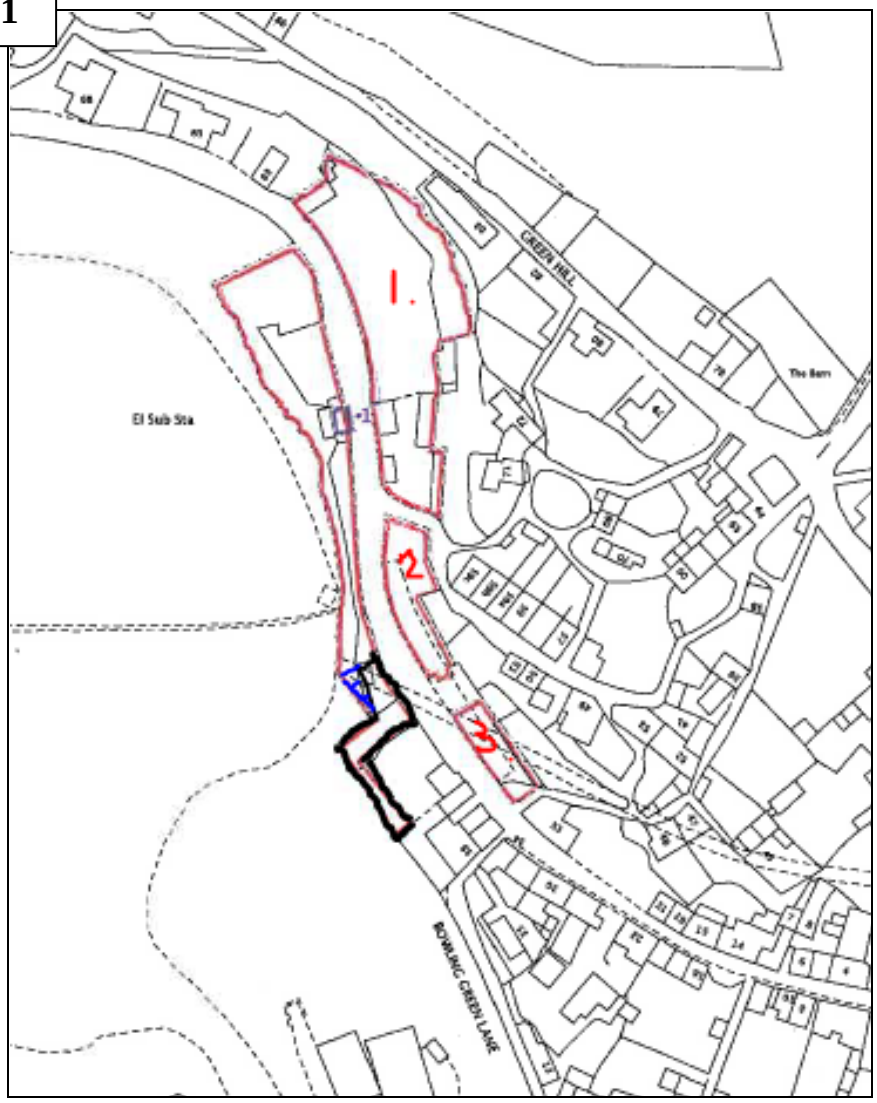
SITE INDEX

SITES IN WHICH INTEREST HAS BEEN EXPRESSED

1. Land at The Dale, Wirksworth
2. Land at Oddfellows, Hathersage – Lease renewal

Land at The Dale Wirksworth

Site No. 1



The area outlined in black is the section being claimed. The area marked in blue is also on the Council's title. Areas 1.2 and 3. are used for parking and a play area.

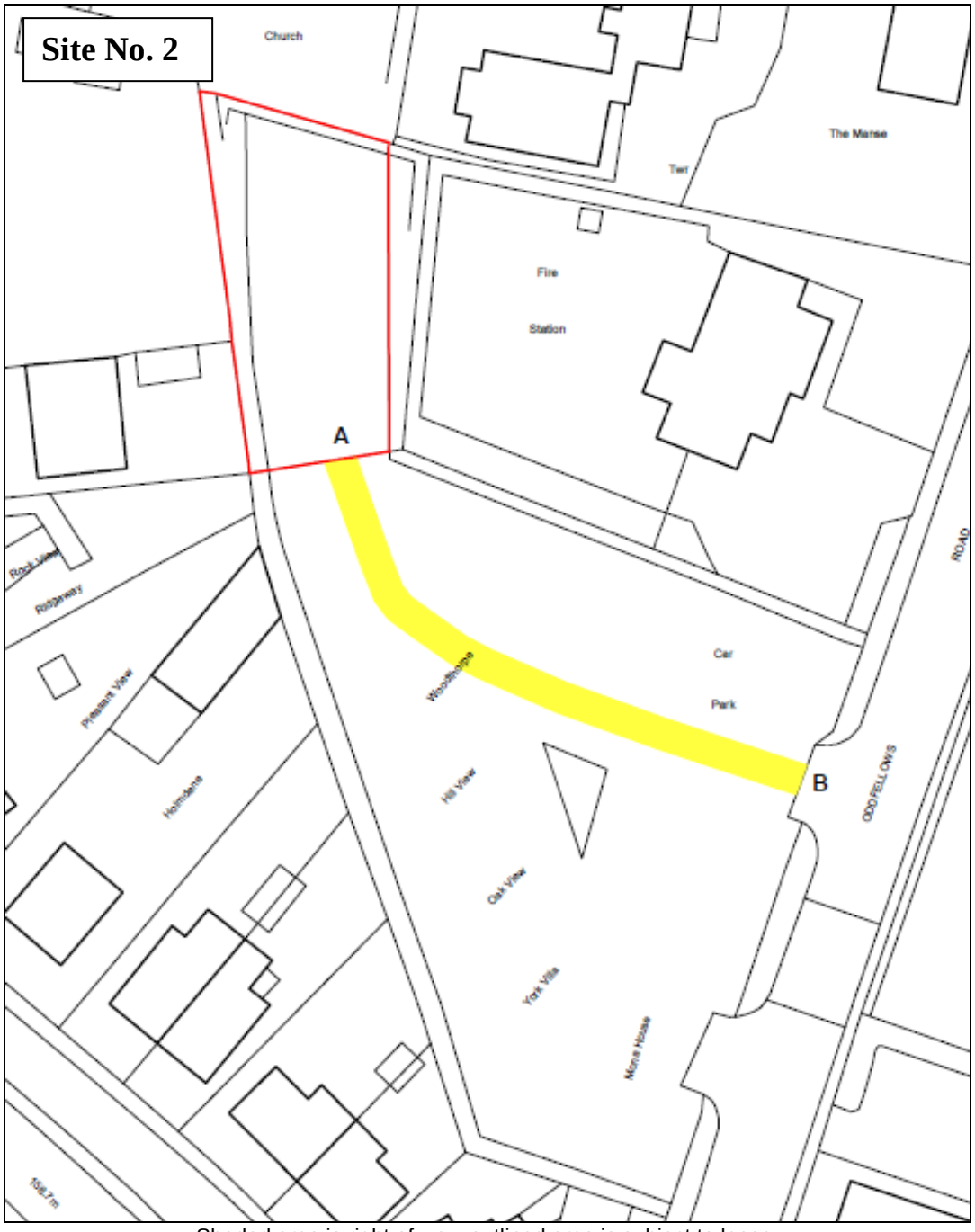
LAND HOLDINGS REVIEW

SITE NO. 1

ADDRESS	Land at The Dale, Wirksworth
REQUEST RECEIVED	An adjoining land owner has expressed an interest in purchasing this land for £1.
DESCRIPTION/LOCATION	This irregular shaped piece of land measures approx. 225m2. It has boundaries between the enquirer's existing property, the quarry face and the road. The land is incorporated into the existing garden and with planning permission a substantial outdoor studio has been constructed. A fenced area to the rear has been used for keeping poultry. This section of the land is above The Dale Tunnel which is entered from the quarry face below.
OWNERSHIP	Derbyshire Dales District Council
LEGAL COVENANTS RESTRICTIONS	The existing covenants relevant to the site will be transferred to the buyer. These are similar to the ones that exist on the buyer's adjoining property.
PLANNING	The buyer will be responsible for obtaining any planning permission.
MAINTENANCE	The site has not been maintained by the Council for considerable time.
HEALTH & SAFETY/RISKS	The boundary to this land is up to the edge of the sheer wall of the quarry. The Dale Quarry Tunnel is below but at considerable depth. This area may provide an important barrier between domestic curtilage and the quarry face.
OFFICER COMMENT	The land appears to have been occupied by the current and previous owner of the adjoining property for a number of years. A statutory declaration is available to confirm this as well as a letter from DDDC to advise that the Council would not object if the previous owners of the neighbouring property put an application in to Land Registry to claim

	the land. The current owners therefore have a strong claim and would be likely to be successful if they put a claim in to Land Registry. The current owners of the adjoining land feel their sale is being delayed because they do not have title to all the land they occupy. In order to progress their sale they have offered to pay a nominal £1 and cover Council costs to secure the land thereby allowing the sale to progress. The alternative is to apply through Land Registry which will cause considerable delay. To improve the Council's boundary it is suggested that the additional triangular piece of land (shaded blue in the plan) also be transferred.
RECOMMENDATION	To proceed with the sale of the freehold of the land for £1, the transfer of existing covenants and purchaser being responsible for any relevant consents and paying £500 legal fees and £100 surveyors fees.

Land at Oddfellows, Hathersage



Shaded area is right of way, outlined area is subject to lease.

LAND HOLDINGS REVIEW

SITE NO. 2

ADDRESS	Land at Oddfellows, Hathersage
REQUEST RECEIVED	A S26 Notice requesting a new lease under the same terms and conditions as existing was received from the tenant.
DESCRIPTION/LOCATION	The site is 490m2 and adjacent to the pay and display car park in Hathersage.
OWNERSHIP	Derbyshire Dales District Council
LEGAL COVENANTS RESTRICTIONS	The Council has a legal obligation under the terms of the lease and current legislation to renew the lease. The tenant could apply to Court if the Council was to withhold renewal.
PLANNING	N/A.
MAINTENANCE	There have been ongoing discussions with the tenant in relation to car park surface, blocked right of way and flooding.
HEALTH & SAFETY/RISKS	None.
OFFICER COMMENT	There are no valid grounds for the Council to object to the lease renewal. As the tenant has rights of renewal based on the existing lease the only terms that can be changed are the rent and any lease modernisations concerning the law. Any other alteration has to be agreed by negotiation.
RECOMMENDATION	To progress lease renewal on commercial terms.

BACK TO AGENDA

NOT CONFIDENTIAL – For public release **Item No. 14**

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Corporate Services & Monitoring Officer

COMPLAINTS MONITORING

PURPOSE OF THE REPORT

This report provides information on formal complaints made under its internal Complaints Procedures; those referred to the Local Government Ombudsman, and against individual elected member behaviour at town, parish and District Council level. The report also recommends an amendment to the Complaints Procedure.

RECOMMENDATION

1. That the report is noted.

2. That the introduction of a time limit for referral of complaints at the final stage of the Complaints Procedure is approved.

WARDS AFFECTED

Various

STRATEGIC LINK

Complaints monitoring has direct links to the Council's core values of fairness and equality, listening to people and quality of service. Additionally it links to the Council's aim of providing excellent services.

---

1. FORMAL COMPLAINTS ABOUT THE DISTRICT COUNCIL'S SERVICES

1.1 Complaints Procedure

This section of the report provides details of complaints against the Council that were dealt with through the Council's Complaints Procedure as formal complaints. During 2016/17 the District Council received 45 official complaints, compared to 33 in the previous year.

The following table shows the number of complaints by service area compared to the previous year.

Service Area	Nature of complaint	2015/16	2016/17
Community Development	Markets	2	0
Community Development -	Leisure	1	5
Corporate Services	Electoral Registration	1	0
Corporate Services	Legal	1	0
Corporate Services	Customer Service	0	2

Service Area	Nature of complaint	2015/16	2016/17
Environmental Services	Refuse collection	5	11
Environmental Services	Car Parks	3	7
Environmental Services	Car parking Permit	0	8
Environmental Services	Public Conveniences	1	2
Environmental Services	Dog Order	1	0
Housing	Allocation	1	0
Regulatory Services	Development Management	12	7
Regulatory Services	Traveller Sites	2	0
Regulatory Services	Environmental Health	0	2
Resources	Benefits	1	0
Resources	Council Tax	1	1
Resources	Estates - Rock Fall	1	0
Total		**33**	**45**

The number of complaints appears to equate to the relative public profile of our services.

Of particular note, it is pleasing that the number of complaints in Development Management is reducing which in some part is undoubtedly due to the progression of the Local Plan.

The increase in complaints regarding car parking is felt to be mitigated now that the new £1 coin and cashless payments are accepted at all car parking machines. The situation will continue to be monitored.

The increase in complaints in the car parking permit are due to a potential flaw in the distribution method by which car parking permits are enclosed with the annual council tax bill. The work is currently outsourced and managed by our Revenues and Benefit partners Arvato. An internal working group has been established to review the process, introduce integrity checks and contractual measures to help improve performance in the future. The Group will also examine alternative means of delivering the benefit of the car parking pass for future consideration by the Council.

The increase in complaints regarding the waste service is considered to be in response to changes in service provision and more active enforcement, which some residents do not like, but which are necessary to deliver the service in accordance with the contract and the District Council's strategy.

For example at the start of 2016 all the 'bring' (recycling) sites were removed following appropriate consultation. During August/September of 2016 the Council began checking holiday lets for premises which may have been using a domestic waste collection in place of the paid for trade service. And, in the summer of 2016 Serco's management structure changed. The new manager, working alongside our own Waste and Recycling Manager have helped to improve performance; introduce default charges for missed bins, and enforce the policy of not accepting side waste and extra bags. Whilst some of these measures are unpopular, they are a contractual part of the service and help to improve our recycling rates.

1.2 **Referral to Chief Executive**

Anyone who is unhappy with the initial response to their complaint can ask for it to be reviewed by the Chief Executive. 13 complaints were referred during the year, which is an increase of 5 from the previous year. The current policy, copy attached as Appendix 1, sets time limits for the District Council's officers to respond at various stages in the complaints process.

1.3 The thoroughness of the final stage in the complaints procedure has a direct correlation to the outcome of complaints that then go onto the Local Government Ombudsman (LGO) as set out below. However, the time limit for complainants to request the independent review can affect the quality of that response in terms of recall of key events. An amendment to the Procedure is therefore recommended as set out below.

1.4 Amendment to Complaints Procedure

The suggested amendments are shown in bold text.

Stage 3 – Review of Formal Complaint

If you are not satisfied with our response, you can ask us to look at your complaint again. The Chief Executive will review it and we will give you our final decision within 20 days of you asking for a review.

You have three months to make your request for a final review unless you have new information which has come to light since you made the original complaint. In requesting a review, please state your reasons or highlight the point(s) you seek to challenge. If your request for a review is beyond the three month time period, please support your request for a review with the new information you wish to be considered.

2 **LOCAL GOVERNMENT OMBUDSMAN**

Complainants who remain dissatisfied with the handling of their complaint following the final stage of the internal complaints procedure may take their issue up with the Local Government Ombudsman (LGO).

The LGO's annual review letter is attached at Appendix 2 and shows that 8 complaints relating to the District Council were received during this period, and 8 decisions were issued which are summarised below. No findings were made against the District Council, which is a significant achievement.

Service	Date	Outcome
Planning & Development	25-Nov-16	Closed after initial enquiries
Housing	03-Jun-16	Advice given
Corporate & Other Services	31-Aug-16	Closed after initial enquiries
Planning & Development	25-Nov-16	Not Upheld
Planning & Development	11-Oct-16	Referred back for local resolution
Corporate & Other Services	02-Dec-16	Closed after initial enquiries
Corporate & Other Services	17-Jan-17	Incomplete/Invalid
Planning & Development	15-Dec-16	Referred back for local resolution

9 complaints were made in the previous 12 month period with one decision upheld.

3. COMPLAINTS ABOUT INDIVIDUAL MEMBER BEHAVIOUR

3.1 The Monitoring Officer received five complaints about individual Member behaviour during 2016/17. One related to a Member of the District Council and four related to parish/town councillors.

3.2 Under the provisions of the Localism Act, the Monitoring Officer is required to assess such complaints against agreed criteria and the relevant authority's Code of Conduct, in consultation with the Independent Person.

3.3 The Assessment involves an examination of the evidence provided with a view to concluding whether on the face it -

(a) the matter falls within the remit of the Code of Conduct. If the answer to this question is 'no', the complaint is immediately dismissed. If the answer is 'yes' the matter proceeds to the next stage;

(b) the potential exists, if proven, for the alleged behaviour to amount to a breach of the District Council's Code of Conduct. If the answer to that is 'No' the complaint is dismissed. If the answer is 'yes', the Monitoring Officer must balance the severity of the potential breach in terms of the public interest in requiring the matter to proceed to a full investigation or to consider whether an alternative remedy is more relevant in the circumstances.

3.4 The complaints received in 2016/17 are summarised on the attached schedule, Appendix 3. The number of complaints overall is similar to those recorded in the previous year with an increased number regarding town and parish council members.

4. CONFIDENTIAL REPORTING POLICY

4.1 The Confidential Reporting Policy, or Whistleblowing Policy, requires the Monitoring Officer to report to the Committee periodically, on matters referred to her under the terms of the Policy. One such matter was referred which subsequently resulted in a disciplinary investigation and dismissal of an employee.

5. RISK ASSESSMENT

5.1 Legal

There was no breach of a rule of law in any of the complaints submitted. For elected Members, Mandatory training is aimed specifically at mitigating the chances of a serious complaint being submitted. The same philosophy is now being rolled out to employees and both Codes of Conduct include attendance at mandatory training.

For town and parish Council issues, the Monitoring Officer has personal responsibility to provide advice on ethical issues and invests time to help parish and town councils develop and mitigate the risk of serious complaints. In the majority of

cases that assistance is welcomed by the parties involved and provides a more cost effective solution to problems. The legal risk continues to be low to medium.

5.2 Financial

There are no financial considerations arising from this report.

6. OTHER CONSIDERATIONS

In preparing this report the relevance of the following factors has also been considered: prevention of crime and disorder, equality of opportunity, environmental, health, legal and human rights, financial, personnel and property considerations.

7. CONTACT INFORMATION

Sandra Lamb, Monitoring Officer, Tel: 01629 761281
e-mail sandra.lamb@derbyshiredales.gov.uk

8. BACKGROUND INFORMATION

None

9. APPENDICES

Appendix 1 - Complaints Procedure
Appendix 2 - LGO Annual review of Decisions 2017
Appendix 3 - Summary of Complaints 2016/17

Complaints Procedure

Improving our Service

At Derbyshire Dales District Council we take pride in the way we deal with our customers. We try and provide you with efficient and high quality services at all times.

We recognise that despite our best efforts sometimes things can and do go wrong. We want to know if you are unhappy or dissatisfied with our service so that wherever possible we can try to put things right.

This procedure sets out how we will –

- Respond to your concerns and complaints regarding our services, and
- Respond to requests for an internal review regarding-
  - Information under the Freedom of Information Act 2000 and
  - Publication Scheme

Our promise to you

We will investigate your complaint promptly and fairly. We will provide you with a full explanation of our investigation into your complaint. There may be occasions when we cannot do what you want but we will try to be as helpful as possible and give you as much information as possible.

What we mean by complaint

We treat a complaint as: an expression of dissatisfaction about our action or lack of action; or dissatisfaction about the standard of service we have provided (or services provided on our behalf).

The Complaints Procedure is not an appeal system to question Council decisions. It is our way of sorting out your dissatisfaction with the services we have or should have provided.

We welcome all types of feedback but not all matters can be handled under this policy. The following types of complaint are excluded from the procedure.

- Planning decisions – unless the complaint relates to the manner in which the complaint was dealt with
- Car parking fixed penalty notices
- Benefit Entitlement
- Complaints that have a legal remedy;
- Complaints about the Conduct of Councillors

If you are unsure who should handle your complaint, please contact the Complaints Officer for Information.

Internal Review of decisions under the Freedom of Information Act

You may request an internal review, if you are unhappy either:

- With the response you received or about any aspect of the way in which requests for information are handled; or
- You consider we are not complying with our publication scheme

The Complaints Officer will acknowledge your request for a review within 5 working days and will aim to send a full response within a further 10 working days.

How the Complaints Procedure works

Stage 1 – Informal Complaint

We will first try to deal with your complaint informally. If you are unhappy about the service you are receiving or have received, then the quickest way to let us know is by contacting the person or service you have been dealing with.

If you have not been dealing with one specific person, then ask to speak to someone in the service area you are concerned with.

You may then be referred to a line manager. You are entitled to speak to a line manager or supervisor and can ask to do this at any time. This person will then try to resolve the issue for you.

Stage 2 – Formal Complaint

This process is used if you are either not satisfied with the results of your informal complaint, or you wish to make your complaint formal from the start.

If so you should make it clear that you want your complaint to be referred to the Complaints Officer. They will ensure that your complaint is investigated and responded to by either the Departmental Director or the relevant Senior Manager, for the service area you have been dealing with.

The Complaints Officer will acknowledge your formal complaint within 5 working days of its receipt and will provide you with the name and contact details of the person dealing with your complaint. We aim to send you a full response within a further 10 working days. If we can’t give you a full response within 10 days, we’ll contact you and explain why.

Stage 3 – Review of Formal Complaint

If you are not satisfied with our response, you can ask us to look at your complaint again. The Chief Executive will review it and we will give you our final decision within 20 days of you asking for a review.

If you're still not happy

Our Complaints Procedure ends at Stage 3. However, if you are not happy, you can take things further by contacting the Local Government Ombudsman. The Ombudsman is totally independent of the District Council and has a legal duty to investigate complaints about local councils.

For more information and details on how to contact the Ombudsman:

Telephone: 0845 6021983

Write to: Local Government Ombudsman
PO Box 4771
Coventry
CV4 0EH

Email: advice@lgo.org.uk

Visit: www.lgo.org.uk

How to contact us with your complaint

You can complain about the services we provide in a number of ways:

- Fill in and return the complaint form in this leaflet
- Fill in the complaint form on the Council website at www.derbyshiredales.gov.uk
- Email your complaint to complaints@derbyshiredales.gov.uk
- Telephone the relevant Council department on 01629 761100 or the Complaints Officer on 01629 761302
- Write to the relevant Council department at the Town Hall, Matlock, Derbyshire. DE4 3NN
- Visit the Council offices in Matlock
- See the Council's website for more details
- Contact your local District Councillor. For more details please contact the Customer Contact Team on 01629 761100 or visit the Council's website.

Formal Complaints in writing

If you wish to make a formal complaint (stage 2 or 3) you will need to put this in writing. This is to make sure we have got the correct details of your complaint before investigating it.

Please be assured that all complaints against the Council are treated in confidence and details are only shared with those who need to know.

All personal details will be held in accordance with the Data Protection Act 1998 and only used in relation to investigating your complaint.

Help filling in the form

If you would like any help or advice in filling in the form please get in touch with an officer in the relevant area or the Complaints Officer.

Unreasonably Persistent Complainants

There are occasions when the behaviour of a small minority of complainants becomes unreasonable, in that they pursue their complaints in a way, which can impede the investigation or can have a significant resource issue for the Council. The Council has adopted an Unreasonable and Persistent Complaints policy to guide both employees and councillors when addressing such complaints. The Complaints Officer will provide a copy of the policy on request.

July 2010

Appendix 2

Local Government & Social Care OMBUDSMAN

20 July 2017

By email

Dorcas Bunton
Chief Executive
Derbyshire Dales District Council

Dear Dorcas Bunton,

Annual Review letter 2017

I write to you with our annual summary of statistics on the complaints made to the Local Government and Social Care Ombudsman (LGO) about your authority for the year ended 31 March 2017. The enclosed tables present the number of complaints and enquiries received about your authority and the decisions we made during the period. I hope this information will prove helpful in assessing your authority's performance in handling complaints.

The reporting year saw the retirement of Dr Jane Martin after completing her seven year tenure as Local Government Ombudsman. I was delighted to be appointed to the role of Ombudsman in January and look forward to working with you and colleagues across the local government sector in my new role.

You may notice the inclusion of the '*Social Care Ombudsman'* in our name and logo. You will be aware that since 2010 we have operated with jurisdiction over all registered adult social care providers, able to investigate complaints about care funded and arranged privately. The change is in response to frequent feedback from care providers who tell us that our current name is a real barrier to recognition within the social care sector. We hope this change will help to give this part of our jurisdiction the profile it deserves.

Complaint statistics

Last year, we provided for the first time statistics on how the complaints we upheld against your authority were remedied. This year's letter, again, includes a breakdown of upheld complaints to show how they were remedied. This includes the number of cases where our recommendations remedied the fault and the number of cases where we decided your authority had offered a satisfactory remedy during the local complaints process. In these latter cases we provide reassurance that your authority had satisfactorily attempted to resolve the complaint before the person came to us.

We have chosen not to include a 'compliance rate' this year; this indicated a council's compliance with our recommendations to remedy a fault. From April 2016, we established a new mechanism for ensuring the recommendations we make to councils are implemented, where they are agreed to. This has meant the recommendations we make are more specific, and will often include a time-frame for completion. We will then follow up with a council and seek evidence that recommendations have been implemented. As a result of this new process, we plan to report a more sophisticated suite of information about compliance and service improvement in the future.

This is likely to be just one of several changes we will make to our annual letters and the way we present our data to you in the future. We surveyed councils earlier in the year to find out, amongst other things, how they use the data in annual letters and what data is the most useful; thank you to those officers who responded. The feedback will inform new work to

provide you, your officers and elected members, and members of the public, with more meaningful data that allows for more effective scrutiny and easier comparison with other councils. We will keep in touch with you as this work progresses.

I want to emphasise that the statistics in this letter comprise the data we hold, and may not necessarily align with the data your authority holds. For example, our numbers include enquiries from people we signpost back to the authority, but who may never contact you.

In line with usual practice, we are publishing our annual data for all authorities on our website. The aim of this is to be transparent and provide information that aids the scrutiny of local services.

The statutory duty to report Ombudsman findings and recommendations

As you will no doubt be aware, there is duty under section 5(2) of the Local Government and Housing Act 1989 for your Monitoring Officer to prepare a formal report to the council where it appears that the authority, or any part of it, has acted or is likely to act in such a manner as to constitute maladministration or service failure, and where the LGO has conducted an investigation in relation to the matter.

This requirement applies to all Ombudsman complaint decisions, not just those that result in a public report. It is therefore a significant statutory duty that is triggered in most authorities every year following findings of fault by my office. I have received several enquiries from authorities to ask how I expect this duty to be discharged. I thought it would therefore be useful for me to take this opportunity to comment on this responsibility.

I am conscious that authorities have adopted different approaches to respond proportionately to the issues raised in different Ombudsman investigations in a way that best reflects their own local circumstances. I am comfortable with, and supportive of, a flexible approach to how this duty is discharged. I do not seek to impose a proscriptive approach, as long as the Parliamentary intent is fulfilled in some meaningful way and the authority's performance in relation to Ombudsman investigations is properly communicated to elected members.

As a general guide I would suggest:

- Where my office has made findings of maladministration/fault in regard to routine mistakes and service failures, and the authority has agreed to remedy the complaint by implementing the recommendations made following an investigation, I feel that the duty is satisfactorily discharged if the Monitoring Officer makes a periodic report to the council summarising the findings on all upheld complaints over a specific period. In a small authority this may be adequately addressed through an annual report on complaints to members, for example.
- Where an investigation has wider implications for council policy or exposes a more significant finding of maladministration, perhaps because of the scale of the fault or injustice, or the number of people affected, I would expect the Monitoring Officer to consider whether the implications of that investigation should be individually reported to members.
- In the unlikely event that an authority is minded not to comply with my recommendations following a finding of maladministration, I would always expect the Monitoring Officer to report this to members under section five of the Act. This is an exceptional and unusual course of action for any authority to take and should be considered at the highest tier of the authority.

The duties set out above in relation to the Local Government and Housing Act 1989 are in addition to, not instead of, the pre-existing duties placed on all authorities in relation to Ombudsman reports under The Local Government Act 1974. Under those provisions, whenever my office issues a formal, public report to your authority you are obliged to lay that report before the council for consideration and respond within three months setting out the action that you have taken, or propose to take, in response to the report.

I know that most local authorities are familiar with these arrangements, but I happy to discuss this further with you or your Monitoring Officer if there is any doubt about how to discharge these duties in future.

Manual for Councils

We greatly value our relationships with council Complaints Officers, our single contact points at each authority. To support them in their roles, we have published a Manual for Councils, setting out in detail what we do and how we investigate the complaints we receive. When we surveyed Complaints Officers, we were pleased to hear that 73% reported they have found the manual useful.

The manual is a practical resource and reference point for all council staff, not just those working directly with us, and I encourage you to share it widely within your organisation. The manual can be found on our website www.lgo.org.uk/link-officers

Complaint handling training

Our training programme is one of the ways we use the outcomes of complaints to promote wider service improvements and learning. We delivered an ambitious programme of 75 courses during the year, training over 800 council staff and more 400 care provider staff. Post-course surveys showed a 92% increase in delegates' confidence in dealing with complaints. To find out more visit www.lgo.org.uk/training

Yours sincerely

Michael King
Local Government and Social Care Ombudsman for England
Chair, Commission for Local Administration in England

Local Authority Report: Derbyshire Dales District Council
For the Period Ending: 31/03/2017

For further information on how to interpret our statistics, please visit our website:
http://www.lgo.org.uk/information-centre/reports/annual-review-reports/interpreting-local-authority-statistics

Complaints and enquiries received

Adult Care Services	Benefits and Tax	Corporate and Other Services	Education and Children's Services	Environment Services	Highways and Transport	Housing	Planning and Development	Other	Total
0	0	3	0	0	0	1	4	0	8

Decisions made

				Detailed Investigations			
Incomplete or Invalid	Advice Given	Referred back for Local Resolution	Closed After Initial Enquiries	Not Upheld	Upheld	Uphold Rate	Total
1	1	2	3	1	0	0%	8

Notes

Our uphold rate is calculated in relation to the total number of detailed investigations.

The number of remedied complaints may not equal the number of upheld complaints. This is because, while we may uphold a complaint because we find fault, we may not always find grounds to say that fault caused injustice that ought to be remedied.

Complaints Remedied	
by LGO	Satisfactorily by Authority before LGO Involvement
0	0

Appendix 3

Summary of Complaints 2016/17

No.	Nature of complaint	Outcome
1	Parish Council complaint regarding two elected Members. Letter purporting to be on behalf of the Parish Council was sent to the local Planning Authority regarding a particular planning application. The contents of the letter were alleged to be contrary to the views of the Parish Council and the two of the three signatories had a conflict of interest in the application which had not been declared.	The assessment was met with a distinct lack of information on the governance structure of the Parish Council, The Parish Council did not have a Clerk; its web site was down and, it seemed that the Parish Council needed help in moving forward. The subject members did not appear to have an understanding of the requirements of them in terms of ethical standards which was compounded by the absence of a Clerk to guide them. It was therefore considered not to be in the public interest to conduct an investigation at cost to the public purse, when a workable remedy appeared more suited to the situation. At the centre of this issue was a planning application which was currently pending at the time of the assessment. To put things right, the recommendations, which were subsequently accepted by the Parish Council were: • That the Parish Council takes immediate steps to withdraw its previous comments on the planning application sent to the Planning Authority and to convene a Special Meeting to formulate a stance on which the majority of parish councillors were agreed. • That the Monitoring Officer be invited to attend the meeting to offer advice on interests in the absence of a parish clerk. • That the Parish Council formally reviews its Code of Conduct and invites the Monitoring Officer to conduct training upon it as soon as practicable.
2	District Council complaint which alleged that the subject member used undue influence to sway the vote on a matter before the Planning Committee.	No evidence was presented to suggest that the subject member may have breached the Code of Conduct and the complaint was dismissed.

No.	Nature of complaint	Outcome
3	Parish Council complaint regarding a letter published by the subject member in the parish magazine. The complaint alleged that the content of the letter may be a breach of the Conduct of Conduct in that the comments may amount to bullying and harassment of an implied party.	No evidence was presented to suggest that the letters published in the parish magazine where in an official capacity as defined in the Parish Council's Code of Conduct. The complaint was dismissed.
4	Town Council complaint which had two limbs concerning one subject member. The first dealt with an exchange of emails between the subject member and the complainant regarding the content of the Town Council's quarterly publication. The complainant claimed that the content of an email sent to her by the subject member, amounted to bullying, contrary to the provisions of the Town Council's Code of Conduct. The second limb of the complaint further alleged that the subject member was also rude to the complainant in Council meetings which may be seen to bring the Town Council into disrepute.	On the first limb the assessment concluded that there is insufficient evidence to point to the potential of a breach of the Code of Conduct with regard to bullying. On the second limb, no evidence was presented to substantiate the claim that the subject member bullied the complainant at meetings of the Town Council and to bring the Town Council into disrepute. The complaint was dismissed on both counts.
5	Town Council Complaint. The complaint concerns alleged bullying of an employee and was made by two separate parties.	The assessment concluded that there was potential for the matter if proven to be a breach of the Code of Conduct. An investigation was initiated which concluded that there was no breach of the Code of Conduct. However, the Town Council is asked to consider the Investigating Officer's recommendations which include the prospect of mediation and for the Council to adopt protocols to support a more productive working relationship between Members and Officers.

BACK TO AGENDA

NOT CONFIDENTIAL – For public release Item No. 15

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Joint report of the Head of Resources and Head of Corporate Services

---

POLICY FOR COUNCIL TAX DISCRETIONARY RELIEF UNDER SECTION 13A (1) (c) OF THE LOCAL GOVERNMENT FINANCE ACT 1992

PURPOSE OF REPORT

To seek approval for the adoption of a policy and the granting of delegated authority relating to Council Tax Discretionary Relief.

RECOMMENDATION

1. That the Policy for Council Tax Discretionary Reliefs under Section13A (1) (c) of the Local Government Finance Act 1992, as set out in the report is approved.

2. That authority is delegated to the Head of Resources and Head of Corporate Services (where primary contact is absent or has a conflict of interest) to reject and approve Discretionary Rate relief in accordance with the policy.

3. That the Chief Executive is delegated authority to determine appeals in accordance with the policy.

WARDS AFFECTED

None

STRATEGIC LINK

The Policy contributes to the delivery of affordable housing: Improve housing for vulnerable people.

---

1 REPORT

1.1 As Billing Authority for Council Tax, the District Council has the right to use the powers set out in Section 13A(1)(c) of the Local Government Act 192 (as amended) to reduce the amount of Council Tax payable. This is a means tested discount aimed at providing assistance to those most in need. To use the legal powers, the Council must set out its policy for administering the scheme.

1.2 A draft Policy which sets out the award criteria and application process is attached at Appendix 1 to the report.

1.3 Decision making is likely to involve a technical assessment of the evidence received against the policy and supporting legislation. As such it is recommended that decision making is delegated to the Head of Resources. The Head of Corporate Services would provide back-up service in the event of holiday absence or where a conflict of interest exists.

1.4 Where the request for relief is unsuccessful or not met in full, the applicant has a right of appeal. Delegated authority is sought for the Chief Executive to review the original decision and consider whether there are grounds to change the decision. The procedure and timescales are set out in the policy.

2 RISK ASSESSMENT

2.1 Legal

The legal basis for the policy is set out in the report. The legal risk is low.

2.2 Financial

Discretionary reliefs under section 13A (1)(c), which replaces the previous 13A discretionary reductions, are borne by the billing authority. As the number of requests is not expected to be significant, the financial risk is assessed as low.

3 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

4 CONTACT INFORMATION

Karen Henriksen, Head of Resources
Telephone: 01629 761284; Email: karen.henriksen@derbyshiredales.gov.uk

Sandra Lamb, Head of Corporate Services
Telephone: 01629 761281; Email: sandra.lamb@derbyshiredales.gov.uk

5 BACKGROUND PAPERS

None

6 ATTACHMENTS

Appendix 1 – Council Tax Discretionary Relief Policy

Policy for Council Tax Discretionary Reliefs
Under Section 13A (1) (C) of the Local Government Finance Act 1992

1. Introduction

1.1 Section 13A (1) (c) of the Local Government Finance Act 1992 (as amended by Section 10 of the Local Government Act 2012) allows the Council (in its capacity as billing authority) to reduce the amount of Council Tax payable to such extent as it thinks fit. This includes the power to reduce the council tax to nil.

1.2 The Council has the right to choose whether to use powers on a case by case basis or to specify a class of use, where several taxpayers may fall into a group due to similar circumstances (e.g. severe flooding). At the present time, the Council has not specified any classes, so all claims will be considered on an individual basis.

1.3 There is a financial implication to awarding reliefs under Section 13A (1) (c) as the Council has to finance all such reliefs from its own funds. Therefore awards must meet the underlying principle of offering value for money to Council Tax payers.

1.4 This policy sets out how Derbyshire Dales District Council will consider applications and apply relief under section 13A (1) (c). This policy applies from 15 September 2017.

2. Purpose of the policy

2.1 This policy outlines the conditions that should be satisfied in order for the Council to consider relief.

2.2 The policy is intended ultimately to enable the Council to provide relief to those in the most extreme financial hardship.

2.3 The Council provides a Council Tax Support (Reduction) (CTS) Scheme in accordance with section 13Aof the Local Government Finance Act 1992. The Council's CTS scheme can be downloaded from the Council's website:

http://www.derbyshiredales.gov.uk/housing-a-council-tax/benefits/council-tax-support

2.4 This discretionary relief policy is independent of the Council's CTS scheme.

3. Award criteria

3.1 Section 13A (1) (c) relief awards will be used in cases of unforeseen or exceptional circumstances that threaten taxpayers' abilities to fund the cost of council tax and may threaten their ability to remain in their homes.

3.2 The main features of this relief are that:

- it is discretionary;
- an applicant does not have a statutory right to a payment;
- the operation of the scheme is for the Council to determine;
- the Council may choose to vary the way in which funds are allocated according to community needs;
- if the applicant is dissatisfied with any decision taken on a claim that they have made, they can ask for further details on the decision and make an appeal in line with Section 5.4 of this Policy.

3.3 Where a scheme relates to a Government Scheme, (e.g. a case of severe flooding) the features of the scheme will be as defined by Government or, where local discretion is allowed, as defined by the Council for that specific instance.

3.4 Derbyshire Dales District Council will consider applying discretionary relief if all of the following circumstances are satisfied:

- The applicant has an outstanding council tax balance;
- There is compelling evidence of extreme financial hardship;
- No other occupants of the property could contribute towards the council tax payable;
- Enforcing the full council tax liability would result in severe hardship e.g. insufficient money being available for basic and essential needs such as housing, food, heating, lighting or essential medical needs;
- The liable person does not have access to assets or funds of any kind which could be used to meet their council tax liability;
- All alternative means of resolving the outstanding liability have been exhausted – this includes but is not limited to discounts, exemptions, council tax support, valuation office/valuation tribunal application;
- The liable person can demonstrate that they have no available income to pay their council tax;
- If the liability relates to a retrospective period the customer can demonstrate and evidence that arrears did not accrue due to their wilful refusal to pay council tax or due to their culpable neglect to pay their council tax.
- The customer can evidence that each of the criteria set out above was satisfied for the entire period for which they wish to be considered for discretionary relief.

3.5 If all of the above circumstances are satisfied the Council will consider granting relief. The Council retains ultimate discretion, in accordance with the discretionary nature of the scheme, and applications for relief will be considered on their individual merits.

3.6 The Council will make all decisions on the basis or merit; it will act fairly and reasonably, and will have regard to all the relevant circumstances.

4. Application Process

4.1 Applications should be made in writing (including email) to the Revenues Team under the title of Section 13A (1) (c) Relief Application. Applications may be made by the customer claiming the reduction, or a party authorised by the applicant.

4.2 Each application must set out the circumstances upon which the application is based and should include:

1. The level of discount being requested (i.e. is this for the full year's council tax or part of it, such as 50%);

2. The reason for the request (i.e. why is the discount wanted and how this meets our policy);

3. Period of time the discount is wanted for (i.e. the full financial year, part of financial year or some other period of time);

4. Steps that have been taken to meet or mitigate the council tax liability (i.e. any other discounts or reductions awarded).

4.3 Where a scheme relates to a Government Scheme, the award of any discount will be as set out by Government or, where local discretion is allowed, as defined by the Council for that specific instance.

4.4 The Council aims to make a decision within 28 days of receiving all the information required.

5. Eligibility Criteria

5.1 Each application will be considered on its individual merits against the conditions set out above.

6. Awarding a Section 13A (1) (c) Relief

6.1 Evidence

In deciding whether to make a Section 13A (1) (c) award the Council will have regard to the applicant's circumstances. In order to do this the Council will make enquiries regarding the income and expenditure of all household members. Household members may be asked to supply reasonable supporting evidence to substantiate the answers that they give to the questions above. This may include, but is not limited to:

- income & expenditure statements;
- any sources of credit such as cash cards, credit cards, store cards, cheque cards, cheque accounts, overdraft facilities, loan arrangements;
- any help which is likely to be available to the applicant from other sources;
- any other special circumstance of which we are aware.

Evidence may be requested that is relevant to the application (e.g. evidence of illness). Where information or evidence requested has not been received within 21 days the Council will determine the application on the basis of the evidence and information in its possession. The Council may refuse to grant relief where the absence of information and evidence prevents the Council from reaching an informed decision regarding the applicant's circumstances.

6.2 Amount of relief

The amount of discretionary relief to be awarded will be at the Council's discretion. Any amount of relief granted will be credited to the council tax account and should not result in a positive balance on the council tax account.

6.3 Period of relief

The Council retains ultimate discretion over the period for which relief may be granted. Relief will only be granted on liability for the financial year in which the request is made or for such prior period as the Council deems appropriate. Relief will not be awarded for subsequent financial years unless a further successful request is made.

The Council retains the right to withdraw relief at any time, including for retrospective periods, if the:

- where conditions or circumstances in which the reduction was granted change or fail to materialise
- information submitted as part of the application proves misleading
- applicant ceases to be a Council Tax payer

The customer must advise the Council of any such relevant change to their circumstances within 14 days of the change occurring.

6.4 Decision making and appeals

Any relief granted in accordance with this policy must be determined as follows:

Decisions for reliefs will be made within 28 days of receipt of application and all relevant information. The applicant will be notified of the decision in writing. The notification will include the decision and details of any amount of relief to be awarded and details of the period to which the award relates.

Where the request for a Section 13A (1) (c) relief is unsuccessful or not met in full the Council will explain the reasons why the decision was made, and explain the applicant's right of appeal.

Section 13A (1) (c) awards are administered under the Local Government Finance Act 1992. Any appeals against a decision to refuse an award or about the amount of any award made will be administered in accordance with the following process:

- An applicant (or their representative) who wants an explanation of a Section 13A (1) (c) Relief application decision may request one in writing within one calendar month of notification of the decision;
- An applicant (or their representative) who disagrees with a decision may appeal the decision;
- Any appeal must be made in writing, but must be made within one calendar month of the original decision being notified to the applicant or, if requested, within one calendar month of the written reasons being notified to the applicant, whichever is the later;
- Where possible the Council will try to resolve the matter by explaining the reasons for the decision to the applicant or their representative either verbally or in writing;
- Where agreement cannot be reached, the Chief Executive will review the decision. The review will be suspended if more information is needed from the applicant;
- The applicant will have one calendar month to respond to the request for further information, thereafter the review will be undertaken on the information held;

Upon receipt of a request for a review, the Chief Executive will review the original decision and consider whether there are grounds to change the decision.

The Council will notify a customer of the appeal decision within 20 days of receiving a request for reconsideration.

The Valuation Tribunal does not have jurisdiction to investigate a Council's decision in respect of section13a discretionary relief in individual cases. In such instances the Valuation Tribunal's opinion is that the Council Tax payer should make an application before the High Court for judicial review.

Where a Council Tax payer is aggrieved by a Council's refusal to abide by its own resolution to award discount regarding a specific class, further appeal may be made to the Valuation Tribunal.

7 Overpayments

7.1 If the Council becomes aware that the information contained in an application for a Section 13A (1) (c) Relief was incorrect or that relevant information was not declared, either intentionally or otherwise, the Council may seek to recover the value of any award made as a result of that application. The award will be removed from the relevant council tax account and any resulting balance will be subject to the normal methods of collection and recovery applicable to such accounts.

8. Fraud

8.1 The Council is committed to the fight against fraud in all its forms. Any applicant who tries to fraudulently claim a Section 13A discount might have committed an offence under the Fraud Act 2006.

8.2 If the Council suspects that fraud may have occurred, the matter will be investigated as appropriate and this could lead to criminal proceedings.

9. Publicity

9.1 The Council will publicise the scheme via their council tax literature and their website, and provide information to relevant agencies, stakeholders and other Council services.

9. Monitoring

9.1 The Council will monitor Section 13A Discount awards to ensure that this policy has been applied fairly and consistently. This monitoring will be conducted by the Revenues Team.

9.2 The Governance and Resources Committee will retain an overview of the policy and will receive an annual report on application of the Policy.

August 2017

BACK TO AGENDA

NOT CONFIDENTIAL – For public release Item No. 16

GOVERNANCE AND RESOURCES COMMITTEE
14 SEPTEMBER 2017

Report of the Head of Resources

APPOINTMENT OF EXTERNAL AUDITOR

PURPOSE OF THE REPORT

At Council in June 2016 Members agreed to opt into the appointing person arrangement being developed by Public Sector Audit Appointments Limited (PSAA) for the appointment of external auditors for the accounts from 2018/19 onwards. PSAA have now made their recommendations on appointments and this report has been prepared as the Council's response to PSAA's formal consultation on the appointment of Derbyshire Dales External Auditor.

RECOMMENDATION

That the PSAA is advised that the District Council has no objection to the appointment of Mazars LLP as the External Auditors from 2018/19 for the next five years.

WARDS AFFECTED

All Wards

STRATEGIC LINK

The services provided under this contract will support the District Council's values to be open and transparent when making decisions and to use public resources ethically and responsibly.

1. BACKGROUND

1.1 Derbyshire Dales District Council has opted into PSAA's auditor appointment arrangements. For audits of the accounts from 2018/19, PSAA is responsible for appointing the Council's External Auditor. PSAA must, under regulation 13 of the Regulations, appoint an External Auditor to each opted-in authority and consult the authority about the proposed appointment. PSAA wrote to the Council on 19 June 2017 to advise that they had completed a procurement to let audit contracts from 2018/19. Mazars LLP was successful in winning one of the contracts in the procurement, and PSAA propose appointing this firm as the auditor of Derbyshire Dales District Council and have now written to the Council to formally consult on this appointment.

2. REPORT

2.1 Attached at Appendix 1 is a copy of the email received from PSAA giving the details of the consultation process and deadlines, and the criteria the Council should consider if it wishes to raise any objections against the appointment of Mazars LLP as the Council's External Auditors for the next five years.

2.2 Having considered these criteria, Officers are not aware of any issues that would result in raising an objection to the appointment of Mazars LLP as the Council's External Auditors and, assuming Members are not aware of any conflicting issues, would recommend acceptance of their appointment.

3. RISK ASSESSMENT

3.1 Legal

The Local Audit and Accountability Act 2014 set out the procedure for the appointment of auditors and Public Sector Audit Appointments Limited has been specified as an appointing person to procure and appoint auditors through a national scheme. The legal risk of implementing the recommendations is assessed as low.

3.2 Financial

The 2017/18 revenue budget includes £48,546 for the appointment of external auditors. It is expected that this provision will be adequate under the new arrangements. The financial risk of implementing the recommendations of this report is assessed as "low".

4. OTHER CONSIDERATIONS

In preparing this report the relevance of the following factors is also been considered prevention of crime and disorder, equality of opportunity, environmental health, legal and human rights, financial personal and property considerations.

5. CONTACT INFORMATION

Karen Henriksen, Head of Resources
Tel: 01629 761284
Email: karen.henriksen@derbyshiredales.gov.uk

6. BACKGROUND PAPERS

None.

7. ATTACHMENTS

Appendix 1 – Consultation email from PSAA

This is a formal communication to the chief executive and chief finance officer of Derbyshire Dales District Council to consult on the auditor appointment from 2018/19

I am writing to consult you on the appointment of Mazars LLP to audit the accounts of Derbyshire Dales District Council for five years from 2018/19. The appointment will start on 1 April 2018.

Background

For audits of the accounts from 2018/19, PSAA is responsible for appointing an auditor to principal local government and police bodies that have chosen to opt into its national auditor appointment arrangements. More information on the appointing person scheme is available on our website.

About the proposed appointment

PSAA must, under regulation 13 of the Regulations, appoint an external auditor to each opted-in authority and consult the authority about the proposed appointment.

Derbyshire Dales District Council has opted into PSAA's auditor appointment arrangements. We have sent regular email communications to audited bodies about this process, and wrote to you on 19 June 2017 to advise you that we had completed a procurement to let audit contracts from 2018/19. Mazars LLP was successful in winning a contract in the procurement, and we propose appointing this firm as the auditor of Derbyshire Dales District Council.

Mazars is a large global audit and accounting firm with over 18,000 professionals in 79 countries worldwide. In the UK the firm ranks in the top ten with 1,700 employees and 140 partners working out of 19 offices, and UK fee income in 2016 of £160m.The firm's dedicated public audit team has significant experience in providing external audit to public sector bodies. It comprises individuals with experience of auditing councils, combined authorities, police bodies, fire and rescue authorities, local government pension funds and other public bodies. In addition to its audit contract with PSAA, the firm also has a substantial portfolio of NHS audits and is one of the National Audit Office's framework suppliers for central government audit.

In developing this appointment proposal, we have applied the following principles, balancing competing demands as much as we can, based on the information provided to us by audited bodies and audit firms:

- ensuring auditor independence, as we are required to do by the Regulations;
- meeting our commitments to the firms under the audit contracts;
- accommodating joint/shared working arrangements where these are relevant to the auditor's responsibilities;
- ensuring a balanced mix of authority types for each firm;
- taking account of each firm's principal locations; and
- providing continuity of audit firm if possible, but avoiding long appointments.

Further information on the auditor appointment process is available on our website.

Responding to this consultation
We are consulting you on the proposed appointment of Mazars LLP to audit the accounts of Derbyshire Dales District Council for five years from 2018/19. The consultation will close at **5pm on Friday 22 September 2017**.

If you are satisfied with the proposed appointment, please confirm this by email to auditorappointments@psaa.co.uk. No further action is needed from you.

The PSAA Board will consider all proposed auditor appointments at its meeting scheduled for 14 December 2017. We will write by email to all opted-in bodies after this Board meeting to confirm auditor appointments.

Process for objecting to the proposed auditor appointment
If you wish to make representations to PSAA about the proposed auditor appointment, please send them by email to auditorappointments@psaa.co.uk to arrive by **5pm on Friday 22 September 2017**.

Representations can include matters that you believe might be an impediment to the proposed firm's independence, were it to be your appointed auditor. Your email should set out the reasons why you think the proposed appointment should not be made. The following may represent acceptable reasons:

1. there is an independence issue in relation to the firm proposed as the auditor, which had not previously been notified to PSAA;
2. there are formal and joint working arrangements relevant to the auditor's responsibilities, which had not previously been notified to PSAA; or
3. there is another valid reason, for example you can demonstrate a history of inadequate service from the proposed firm.

We will consider carefully all representations and will respond by Monday 16 October 2017 by email.

If your representations are accepted, we will consult you on an alternative auditor appointment between 16-27 October 2017. If your representations are not accepted, we will confirm this to you. You may choose to make further representations to the PSAA Board, providing any additional information to support your case.

We will write to all bodies to confirm the Board's final decision on the appointment of the auditor before 21 December 2017.

Scale fees for 2018/19
We will consult on scale fees for 2018/19 in due course and will publish confirmed scale fees for 2018/19 for opted-in bodies on our website in March 2018. The results of the audit procurement indicate that a reduction in scale fees in the region of approximately 18 per cent should be possible for 2018/19, based on the individual scale fees applicable for 2016/17. Further information on the audit procurement is available on our website.

Further information
If you have any questions about your proposed auditor appointment or the consultation process, please email us at auditorappointments@psaa.co.uk.

Yours sincerely

Jon Hayes
Chief Officer

BACK TO AGENDA