OPEN REPORT
GOVERNANCE AND RESOURCES COMMITTEE

Governance and Resources Committee – 14 September 2023

DATA PROTECTION AND INFORMATION GOVERNANCE ANNUAL REPORT 2022/23

Report of the Director of Corporate and Customer Services (Monitoring Officer)

Report Author and Contact Details
James McLaughlin, Director of Corporate and Customer Services
01629 761281 or james.mclaughlin@derbyshiredales.gov.uk

Mark Mealey, Information Governance Officer
01629 761396 or mark.mealey@derbyshiredales.gov.uk

Caroline Leatherday, Business Support Manager
01629 761105 or caroline.leatherday@derbyshiredales.gov.uk

Wards Affected
District-wide

Report Summary
This report is an annual report on the Council's compliance with the General Data Protection Regulation, the Data Protection Act and the Freedom of Information Act.

Recommendation

That the Data Protection and Information Governance Annual Report 2022/23 be accepted.

List of Appendices
None

Background Papers
Nil

Consideration of report by Council or other committee
Not applicable

Council Approval Required
No

Exempt from Press or Public
No

Data Protection and Information Governance Annual Report 2022/23

1. Background

1.1 The function of Information Governance supports the Council's compliance with the General Data Protection Regulations GDPR (UK GDPR), Data Protection Act (DPA) 2018, Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (EIR). The Council has a statutory obligation to comply with the IG framework by responding appropriately to requests and managing personal data lawfully. Officers within the Corporate and Customer Services department assist the organisation by monitoring internal compliance, informing and advising on data protection obligations, providing advice and guidance and raising awareness on data protection matters.

1.2 FOIA/EIR impose a statutory obligation on the Council to respond to requests for information within 20 working days, subject to relevant exemptions. The Code of Practice, issued by the Secretary of State for Constitutional Affairs under Section 45 of the FOIA, requires public authorities to have a procedure in place to deal with complaints in regard to how their requests have been handled. This process is handled by the Information Governance Team as an FOI/EIR internal review. After an internal review has been completed an applicant has a right to complain to the Information Commissioner's Office (ICO) for an independent ruling on the outcome. Based on the findings of their investigations, the ICO may issue a Decision Notice. The ICO may also monitor public authorities that do not respond to at least 90% of FOI/EIR requests they receive within 20 working days.

1.3 The DPA 2018 provides individuals with the right to ask for information that the Council holds about them. These are also known as Subject Access Requests (SARs). The Council should be satisfied about the individual's identity and have enough information about the request. The timescale for responding to these requests is one month, starting on the day of receipt. Authorities can extend the time taken to respond by a further two months if the request is complex or a number of requests have been received from the individual, e.g. other types of requests relating to individuals' rights.

1.4 There is no requirement for the Council to have an internal review process for SARs. However, it is considered good practice to do so. Therefore, the Council informs applicants of the Council's internal review process. However, individuals may complain directly to the ICO if they feel their rights have not been upheld.

1.5 The Council's management of data protection security incidents is undertaken by the Information Governance Officer on behalf of the Data Protection Officer (DPO), who records, investigates and where necessary, recommends actions to be taken based on the impact risk level.

1.6 Monitoring of the Council's compliance with GDPR and DPA is carried out by the Information Governance Board which is chaired by the Council's Data Protection Officer. The Director of Corporate and Customer Services became the Data Protection Officer in December 2022, taking on the

responsibility from the Director of Resources following a reallocation of responsibilities. Any risks relating to Information Governance, including GDPR and Data Protection are monitored on a regular basis by this group. Risks and actions are logged and reviewed at Information Governance Board meetings and, if necessary, are escalated in line with the Council's risk management processes.

1.7 The regulator for information in the UK is the Information Commissioner's Office (ICO), which is "an independent body established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals". Part of the ICO's role is thus to hold organisations to account for the way they manage their information. As an organisation that processes personal data, the Council is required to register with the ICO, and pay an annual fee. The Council's Data Protection Registration Number is Z6752355, and the current registration expires on 15 May 2024.

2. Key Issues

Performance

2.1 Performance reporting is an important part of helping to ensure that the Council is monitoring the effectiveness of its information governance arrangements, and its compliance with legislation.

2.2 There are a number of performance indicators that are measured and regularly reported to the Information Governance Board:

Performance Indicator	**2020/21**	**2021/22**	**2022/23**
Number of Security Incidents reported (all incidents)	33	25	8
Number of data breach notifications to the ICO	0	0	0
Number of Subject Access Requests (SARs) received	10	7	7
Number of open SARs	0	0	0
Number of overdue SARs	0	0	0
% of SARs responded to within statutory timescales	100%	100%	100%
Third Party Requests (e.g. Proof of Life, CCTV, DWP, HMRC, Local Authorities etc)	16	16	14
Number of Information Requests (FOI/EIR) received	621	662	716
% of Information Requests responded to within statutory timescales	98%	99%	99%

2.3 There is a lack of benchmarking information available regarding information governance matters. The Council is not required to submit any annual returns to the Information Commissioner's Office or any other body, and there is therefore no published data that can help the Council assess how it compares to other similar authorities. The ICO has stated its intention to

publish statistical information at some point, but there are no timescales associated with this at the current time.

Training and Awareness

2.4 It is critical that all Council staff understand the importance of dealing with the Council's information appropriately, safely and securely. Getting it right means the personal information the Council holds about customers and citizens, and the Council's own information, is protected.

2.5 The ICO requires all staff to undertake mandatory data protection training at least every two years. Since this requirement has been in place, the District Council has used an e-learning training package. This has the advantage of ensuring that the content is directly relevant to Council staff.

2.6 In addition to formal training, awareness-raising is also a valuable way of keeping staff appraised of information governance matters. There are various mechanisms available to facilitate this, including: publishing information governance advice and guidance on the Council's intranet, which is updated and expanded regularly.

2.7 Information governance training, covering data protection and Freedom of Information, is also provided to all District Councillors by the Information Governance Team following an election. All 34 District Councillors were invited to training on 25 July, which was recorded and made available to all Members after this date. This training followed the Council elections in May 2023 as part of the induction programme, and individual sessions for any Member can also be provided as required.

Information Security Incidents and Personal Data Breaches

2.8 Confidentiality and security of information about service users and citizens is extremely important, and the Council has robust policies and processes in place to minimise the risks associated with collecting, storing and managing vast amounts of information.

2.9 Some information security incidents result in a personal data breach, which occurs when personal or 'special category' data is lost, damaged or destroyed, either accidentally or on purpose; and/or shared with, or accessed by, someone who is not entitled to access it, either accidentally or on purpose.

2.10 The UK GDPR states that where a personal data breach incident is likely to result in risk of harm to the rights and freedoms of individuals, the Council must inform the ICO within 72 hours of becoming aware of the breach. This requires the use of the ICO's standard notification form. The Council also has a lawful duty to inform the individuals affected without undue delay if a breach is likely to result in high risk to their rights and freedoms.

Individuals' Rights

2.11 UK Data Protection law provides a number of rights for individuals in relation to the personal data that an organisation holds about them, namely:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

2.12 Under data protection legislation, the Council must give individuals the right of access to their personal information under the 'right of access'. An individual can submit a Subject Access Request (SAR) requiring the Council to provide them with a copy of any personal information which it holds about the individual. The right of access to records can also be exercised by an authorised representative on an individual's behalf (for example, a solicitor). The Council has one month to respond to a valid SAR, although this can be extended by two months for requests where the records are deemed to be voluminous and/or complex.

2.13 Since 2018 increased awareness of the rights of individuals to access information about themselves has resulted in a significant increase in the number of SARs submitted to the Council in recent years. This has resulted in Information Governance Officer spending significant time and resource to ensure statutory deadlines are complied with.

2.14 Since GDPR has been in force, there have been a number of requests from individuals exercising rights (other than the right of access referred to above), relating to their personal data. Particularly, there has been an increase in terms of requests under 'the right to erasure' (also known as the 'right to be forgotten'), and 'the right to rectification' (of inaccurate or incomplete information). The Council has one month to respond to such requests, and these are actioned by services where it is appropriate to do so.

	Number of requests	
Type of request	**2021/22**	**2022/23**
Request to erasure	0	0
Request to rectification	3	1
Request to restrict processing	0	0
TOTAL	3	1

Freedom of Information

2.15 The Freedom of Information (FOI) Act 2000 provides a general right of access to recorded information held by any public authority. The Environmental Information Regulations (EIR) 2004 provide a similar right of access to environmental information held by public authorities.

2.16 Requests received by the Council under FOI or EIR regimes have similar obligations and are handled in a similar way. Anyone can make a request, and the Council receives requests from a wide variety of sources, including

individual citizens, organisations, media organisations, political organisations and legal bodies.

2.17 The process for handling FOI and EIR requests is co-ordinated by the Council's Business Support Team, with relevant services providing the information for the response to the request.

2.18 In the last three years, the District Council has managed the following numbers of requests under FOI and EIR:

	2020/21	**2021/22**	**2022/23**
Total number received	621	661	716
Total responded to by the District Council	529	569	600
Number re-directed to Derbyshire County Council	85	89	109
Number withdrawn	7	3	7
Number covered by an exemption	37	41	17
Number of Internal Reviews for FOI responses received	3	1	6

2.19 Under the legislation, the Council must respond to all FOI/EIR requests for information within 20 working days. Failure to comply with this deadline could lead to a complaint by a specific requestor to the Information Commissioners Office (ICO). The ICO has the power to serve a Decision Notice on a public authority for failing to comply with the 20-working day deadline.

2.20 The ICO's expected minimum level of compliance with responding to FOI and EIR requests is 90%. As the table below shows, the Council has exceeded this target in each of the last three years.

2.21 If a requester is not satisfied with the response to their FOI/EIR request, they can request an Internal Review of the response. In 2022/23, 6 such reviews were requested, which equates to 0.8% of the total requests received. In 6 cases, the review upheld the Council's original response, 0 cases were partially upheld and 0 were overturned. 0 complaints were lodged with the ICO.

Priority Activities for 2023-24

2.22 Listed below is a summary of some of the main developmental activities that are planned for 2023/24. Progress against these actions will be reported in the Annual Report for 2023/24:

- Improve the Council's compliance with the ICO Accountability Tracker – this will be a key task for the new Director of Corporate and Customer Services in their capacity as the authority's Data Protection Officer

- Review and update the Council's Information Asset Register and Records of Processing Activities to take account of new processes and systems
- Review and update the Council's suite of information governance policies to reflect organisational changes and wider national developments
- Further develop the 'self-service' approach to information management advice and guidance via the Council's intranet
- Implement additional measures to seek to minimise the number of security incidents occurring, including targeting additional training for those services where incidents are most prevalent
- Work collaboratively across services to maintain the Council's high compliance rate for Subject Access Requests (SARs)

3. Options Considered and Recommended Proposal

3.1 There are no new proposals or recommended options. However, it is a requirement that the Council continues the maintenance of its Information Governance policies and processes in compliance with Data Protection requirements.

3.2 It should be noted that continued compliance to GDPR and the Data Protection Act 2018 can only be achieved by the continued support of all Council staff and Councillors. Key roles such as Information Asset Owners and Data Protection Officer can use existing governance structures to ensure ongoing compliance.

3.3 It is essential that the Council continues to monitor and report on its performance in relation to access to information requests, information security incidents and training completed in order to promote best practice information governance and drive continuous improvement in the Council's ability to comply with the laws relating to information.

4. Consultation

4.1 There are no proposals for decision within this report so there has been no need to consult on the content of the paper.

5. Timetable for Implementation

5.1 There are no proposals for decision within this report so there is no timetable for implementation.

6. Policy Implications

6.1 There are no direct policy implications arising from this report. However, ensuring the Council's information governance policies are kept up to date and relevant is a critical element in ensuring the Council is compliant with all relevant legislation and changes in the national policy landscape.

6.2 The Council has a comprehensive suite of information and IT security policies, all of which are published on the Council's website, and all policies are reviewed every two years as a minimum. A review of all policies will be

undertaken within three years of adoption, with any significant revisions approved by the Information Governance Board.

6.3 The monitoring and reporting of the Council's performance regarding responding to, and handling access to information requests under FOIA and DPA 2018, including any complaints made to the ICO will enable continuous improvement, raise awareness and promote high standards of information governance, fostering a culture of openness and transparency within the Council and demonstrating our commitment to best practice information governance, security, and protection.

7. Financial and Resource Implications

7.1 There are no direct financial or resources implications directly arising from this report.

8. Legal Advice and Implications

8.1 There are no legal implications arising from this report, except to reiterate that the council has a duty to comply with Data Protection legislation.

9. Equalities Implications

9.1 There are no direct equalities implications arising from this report.

10. Climate Change and Biodiversity Implications

10.1 There are no direct climate change or biodiversity implications arising from this report.

11. Risk Management

11.1 Risks and mitigation will be managed by Information Governance Board, the Corporate Leadership Team and the council's risk processes. There are three principle risks that are monitored regularly:

(a) The growth in the number of security incidents occurring throughout the Council could lead to the greater loss of sensitive information and a corresponding rise in data breaches involving sensitive personal information, resulting in harm to citizens, damage to the Council's reputation and the imposition of sanctions from the Information Commissioner's Office.

(b) The continued growth in the volume and complexity of Subject Access Requests (SARs) from individuals wishing to access their personal data has resulted in a significant increase in workload for the Information Governance Officer. This increase impacts on their capacity to undertake other parts of their role, which in turn increases the risk of issues arising.

(c) There is a risk the Council could be subject to a major cyber security attack or information breach resulting in financial loss, significant disruption to services, and reputational damage.

Report Authorisation

Approvals obtained from Statutory Officers:-

	Named Officer	**Date**
Chief Executive		
Director of Resources/ S.151 Officer (or Financial Services Manager)	Karen Henriksen	25/08/2023
Monitoring Officer (or Legal Services Manager)	James McLaughlin	06/09/2023