SANDWELL MBC
SIRO REPORT
2023/2024

CONTENTS

1. Purpose of the Report 3
2. Introduction 3
3. Current Information Governance Structure 3
3.1 Senior Information Risk Officer (SIRO) – Alex Thompson 3
3.2 Caldicott Guardian – Trudie Morris 3
3.3 Data Protection Officer (DPO) – Vanessa Maher-Smith 4
3.5 Information Governance Team (Governance Team) 4
3.6 Service Areas and Information Asset Owners (IAO) 4
3.7 Managers 4
3.8 Officers and Employees 5
4. Information Governance Board 5
5. Changes to Legislation During Reporting Period 5
6. Key Projects 5
7. Data Breach Incidents 7
7.1 Data Breaches 7
7.2 Data Breach Claims 9
8. Requests for Information under Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR) 9
9. Data Subject Access Requests 9
10. Complaints raised to the Information Commissioner 10
11. Appeals to the Information Rights Tribunal 11
12. Data Security Protection Toolkit (NHS Toolkit) 11
13. Information and Cyber Security 13
14. Awareness and Training 13
15. Priorities for 2024-2025 14

1. Purpose of the Report

This report provides an overview of Sandwell MBC's adherence to regulatory requirements relating to the processing of personal data under the UK General Data Protection Regulation (UK UK GDPR) and the Data Protection Act 2018.

2. Introduction

Until December 2023 the responsibilities of the Senior Information Risk Officer were discharged by the Council's Director of Law and Governance. As of 7th May 2024, the Executive Director for Finance and Transformation assumed this responsibility.

The SIRO has overall responsibility for the Council's information governance framework and acts as the lead for information risk within the Council. The SIRO is responsible for producing an annual report on information governance.

This annual report provides an overview of activity in relation to information governance, key achievements during 2023/24 as well as outlining work planned for 2024/25.

3. Current Information Governance Structure

Within the Council the responsibility for Information Governance sits with all staff at all levels. However, there are certain individuals who have specific responsibilities, summarised below:

3.1 Senior Information Risk Officer (SIRO) – Alex Thompson

The SIRO will:

- Oversee the development of an Information Risk Policy, and a strategy for implementing the policy within the existing Information Governance framework.
- Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk
- Review and agree action in respect of identified information risks.
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and / or discussion of information risk issues.
- Ensure the board is adequately briefed on information risk issues.
- Ensure that all care systems information assets have an assigned Information Asset Owner.

3.2 Caldicott Guardian – Trudie Morris

The Caldicott Guardian will:

- Ensure that the personal information about those who use its services is used legally, ethically and appropriately, shared where appropriate and that confidentiality is maintained.

- Act as the link between social care activities, the Information Governance Team and Information Governance Board ensuring policies and procedures are embedded within their service areas.

3.3 Data Protection Officer (DPO) – Vanessa Maher-Smith

The DPO will:

- Inform and advise the Council about complying with UK GDPR and other data protection laws.
- Monitoring compliance with UK GDPR and data protection laws – including staff training and internal audits.
- Advise on and monitor data protection impact assessments.
- Be the point of contact for the ICO
- Be the point of contact for Data Subjects

3.5 Information Governance Team (Governance Team)

The Governance Team will:

- Act as a point of contact for advice and guidance.
- Be responsible for the development and promotion of Information Governance policies and guidance within the Council.
- Ensure that the Council maintains its notification to the ICO and will act as the key contact point between the Council and ICO.
- Support the roles of the SIRO and DPO in meeting their obligations on a day to day basis.

3.6 Service Areas and Information Asset Owners (IAO)

- Each service area will nominate an appropriate IAO to undertake information governance processes and activities deployed within their service
- The IAO will undertake and co-ordinate tasks, in association with the IG Team, e.g information asset register

3.7 Managers

- Managers are responsible for ensuring their officers are informed of policies, support procedures and provide adequate time to undertake training offered by the Council. They must ensure that their officers understand and adhere to policy and procedure whilst undertaking their work functions
- All Managers must inform the Governance Team of any security incidents, data losses or other DPA breaches;
- Managers must ensure that their Officers undertake all relevant information governance training related to Data Protection including refresher training where appropriate

3.8 Officers and Employees

- All Officers and Employees (permanent, temporary or agency) have a responsibility for abiding by UK GDPR and the DPA and adhere to the Council's policies and procedures.
- All mandatory training offered must be taken up whilst appropriate, relevant additional training must also be considered e.g. SAR training for Officers routinely involved with the handling of such requests
- All Officers must report actual or suspect security incidents, data losses, breaches to their Manager and the Governance Team following the Council process.

4. Information Governance Board

The Council has its own Information Governance Board, which under the leadership of the Senior Information Risk Owner and Data Protection Officer maintains oversight of the Council's compliance with UK GDPR and Data Protection legislation. There are representatives from each service area across the Council to ensure information is collated and disseminated as necessary.

The Terms of Reference for the Board were reviewed in March 2024 and a final updated version was approved in May 2024. A copy of the Terms of Reference is attached as Appendix 1.

5. Changes to Legislation During Reporting Period

There are no significant changes to legislation during the reporting period.

6. Key Projects

6.1 Review of the Council's compliance with the Transparency Code

In 2015 the Government issued the 'Local Government Transparency Code 2015'. The purpose of the Code was to meet the government's desire to increase democratic accountability and make it easier for local people to access information and contribute to local decision making and shape public services.

The Code sets out:

- Information that councils must publish; and
- Information that it recommends that councils should publish.

A full review of the Council's compliance with the Transparency Code was completed. This resulted in an update of the Council's internet page to single page that demonstrates compliance with the Code and links to all of the information published under the Code by the council:

https://www.sandwell.gov.uk/council/publication-scheme

The updated website was presented to IGB on 8th December 2023 and approved.

6.2 Review of Retention Schedule

A full review of the Council's Retention Schedule was completed by the Governance Team through IGB members in March 2023/April 2023.

The updated Retention Schedule was approved by IGB on 21st April 2023. It was approved by Cabinet on 13th September 2023 and is now available on the Council's internet page:

https://www.sandwell.gov.uk/downloads/download/454/sandwell-council-retention-policy

This included a risk assessment in relation to the retention and deletion of emails in relation to the Council's requirement to retain all information that may be required for the purpose of the Covid 19 Inquiry. The retention period for emails is 8 years, and the Council intends to set this up automatically, rather than expecting staff to manually delete emails. As such, a process has been established to ensure that any Covid-19 related data is retained.

6.3 Review of Privacy Notices

A full review of the Council's Privacy Notice was completed by the Governance Team through IGB members. This involved all IGB members liaising with their service areas to ensure that the information relevant to their services was included in the corporate Privacy Notice.

The final version was approved by IGB on 10th November 2023 and was made available on the Council's Internet Page:

https://www.sandwell.gov.uk/privacynotice

IGB members also encouraged individual service areas to review their own Privacy Notices, where they had local versions specific to certain processing arrangements. The following Privacy Notices were also updated as part of this process:

- Social Housing De-Carbonisation Fund
- Sandwell Safeguarding Adult Board (SSAB)
- Healthy Sandwell
- Domestic Homicide Reviews

6.4 Policy Reviews – Information Governance Framework and Information Right's Policy

Full reviews were conducted of the Council's key Information Governance Policies.

The Information Governance Framework is the Council's internal policy for staff. It was reviewed and approved by IGB on 10th November 2023. It was circulated to Leadership Team on 11th December 2023 for approval.

The Information Rights Policy is the Council's public policy. It was circulated to Leadership Team on 11th December 2023 for approval and was approved by Cabinet on 17th January 2024.

6.5 Information Asset Register Reviews

Information Asset Registers were reviewed throughout 2024.

This is an ongoing requirement to ensure they are updated regularly and in particular when there are changes in location of data and staffing.

7. Data Breach Incidents

7.1 Data Breaches

Between April 2023 and March 2024 225 data breach reports were sent through to the Information Governance Team. Of those, after investigation, 211 were confirmed as being data breaches.

This compares to 209 in the period April 2022 to March 2023.

Breaches according to Directorate:

Directorate	Total
Housing	49
Adult Social Care	37
Finance	36
Law and Governance	29
Children and Education	28
Borough Economy	23
Business Strategy and Change	15
Public Health	3
Regeneration and Growth	3
Unknown	2
Total	**225**

Causes of breaches:

Brief Description of Breach	Total
External - Information emailed to incorrect recipient	38
Internal - Information emailed to incorrect recipient	31
Postal - Sent to Wrong Address	30
Unauthorised Disclosure to Third Party	22
Loss / Theft of Equipment	19
Postal - Incorrect Information Sent	19
NA - No Breach	14
Unauthorised Access	10
External - Incorrect Information emailed	9
Failure to Redact	9
Internal - Incorrect information emailed	8
Information Left in Insecure Location	6
Unknown	4
Loss / Theft of Paperwork	3
Failure to Use Bcc	1
Rent Calling Card Issued to Incorrect Address	1
Verbal Disclosure of Personal Data	1
Total	**225**

The council reported one data breach to the ICO during 2023/24 which related to the worldwide cyber attack on MOVEIT. The Council's MOVEIT system was not affected, but one of the Council's Data Processors was and Council data was compromised. The ICO took no action, but recommended that the Council reviews it's contracts with all Data Processors. This action is being taken forward into 24/25.

7.2 Data Breach Claims

Between April 2023 and March 2024 the Council received 2 civil claims for compensation relating to data breaches. No damages were paid in either case by the Council.

8. Requests for Information under Freedom of Information Act (FOIA) and Environmental Information Regulations (EIR)

For the period March 2023 – April 2024 the council received a total of 1144 requests for information under FOIA and EIR. Of those, 85% were answered within the statutory period.

This compares to 76% in the period March 2022 to April 2023.

The statutory period for compliance for requests under FOIA is 20 working days. In specific circumstances where the council is seeking to apply an exemption that requires consideration of the Public Interest Test, the council may extend the timescale until such time as is reasonable in the circumstances (the ICO guidance is that this should be a maximum of a further 20 working days).

The statutory period for compliance for requests under EIR is 20 working days. In specific circumstances where the council is seeking to apply an exemption that requires consideration of the Public Interest Test, the council may extend the timescale by a further 20 working days.

The breakdown by Directorate is:

Directorate	Timescale Met	Timescale Missed	Open & In Timescale	Total Received	Compliance
Regeneration and Growth	104	2	0	106	98%
Public Health	28	1	0	29	97%
Law and Governance	47	3	0	50	94%
Business Strategy and Change	100	7	0	107	93%
Borough Economy	290	21	0	311	93%
Corporate Enquiries	37	3	0	40	93%
Finance	115	26	0	141	82%
Housing	108	29	0	137	79%
Children and Education	91	44	0	135	67%
Adult Social Care	54	34	0	88	61%
Total	**974**	**170**	**0**	**1144**	**85%**

The Council's target is 95% compliance with the statutory time limits under FOIA and EIR. Performance will continue to be monitored and steps taken to ensure improved performance.

9. Data Subject Access Requests

Between April 2023 and March 2024 the Council received 220 Subject Access Requests (SAR). Of those, 71.56% were answered within the statutory period.

This compares to 60% for the period April 2022 to March 2023.

Under UK GDPR a SAR must be responded to within one calendar month. There is scope for this to be extended by a further two months where a request is complex or where an individual has made a number of requests eg erasure, rectification.

Directorate	Timescale Met	Timescale Missed	Other	Total Received	Compliance
Regeneration and Growth	2	0	0	2	100.00%
Law and Governance	9	1	0	10	90.00%
Business and Strategy	16	2	0	18	88.89%
Housing	71	9	3	83	88.75%
Borough Economy	15	3	0	18	83.33%
Corporate Enquiries	3	1	0	4	75.00%
Housing - HDR	7	6	3	16	53.85%
Finance	10	9	0	19	52.63%
Children and Education	9	11	1	21	45.00%
Adult Social Care	9	18	2	29	33.33%
Total	**151**	**60**	**9**	**220**	**71.56%**

The Council has had a number of challenges to its compliance with SARs over this period.

Firstly, there has been a significant increase in SARs in the Housing Directorate directly as a result of the Housing Disrepair Claims. In summary, there has been an increase in the volume of Housing Disrepair claims received by the Council in relation to it's housing stock. As part of the legal pre-action protocol, claimants are entitled to seek disclosure of relevant information. Due to the volume of requests, the Council was unable to meet the timescales for providing disclosure in compliance with the pre-action protocol and as such claimants resorted to making Subject Access Requests for their tenancy files in order to obtain their personal information. A process has now been put in place and increased resources to ensure compliance with the pre-action protocol, thereby reducing the volume of SARs received.

In relation to the Adult Social Care SARs, it is recognised that they are significant in both volume and complexity. Dealing with these SARs takes a lot of officer time as the following tasks are required:

- extract the information from the LAS system,
- redact the information applying relevant exemptions in accordance with legislation
- obtain approval of the relevant AD

Various options have been explored to improve compliance and whilst some have resulted in short term success, consideration needs to be given to a more long term resolution. Discussions are ongoing in relation to a redaction tool that may provide support.

10. Complaints raised to the Information Commissioner

There were 12 complaints to the ICO as follows:

- 5 stating they were unhappy with the response received in relation to their request for information under FOIA/EIR. Of those:
    - 1 was closed with no further involvement as the Council provided an updated response to the requester.
    - The ICO issued Decision Notices on 2 cases, upholding the Council's position.
    - The ICO issued a Decision Notice on 1 case, upholding the Complainant's position and requiring the Council to disclose information.
    - 1 remains pending.

- 6 stating that they had not received responses to their Subject Access Requests within the statutory timescales. They were all closed with no further action, as either the Council had subsequently complied with the response, or it did so within the timescales set by the ICO.

- 1 complaint about the way the council had dealt with an individual's data. This was resolved with no further action.

11. Appeals to the Information Rights Tribunal

In the period 23/24 the Council dealt with 5 Appeals to the Information Right's Tribunal. Of those:

- 2 were withdrawn by the Appellant
- 1 was dismissed by the Tribunal
- 2 remain pending

12. Data Security Protection Toolkit (NHS Toolkit)

The Data Security and Protection Toolkit is an online self assessment tool that allows organisations to measure performance against the National Data Guardian's 10 Data Security Standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and the personal information is handled correctly.

The toolkit is grouped under three leadership obligations to address people, process and technology issues:

Leadership Obligation 1: People

People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process

Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology

Technology: ensure technology is secure and up to date.
Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.
Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

The Governance Team worked with ICT, Business Continuity Leads, and IGB Members to ensure that the 2022-23 DSPT was completed by 30 June 2023. The Council achieved a 100% rate, which equates to an overall "Standards Met" assessment position.

13. Information and Cyber Security

The risk of Cyber Security and Information Governance (IG) in terms of data is still a major risk consideration to any organisation.

The SIRO is supported by the Assistant Director for ICT and the Council's dedicated Cyber Security Team within ICT Services who are responsible for the integrity and protection of the Council's network, systems and data.

14. Awareness and Training

The following training is made available to all Council officers:

- Mandatory Data Protection and Cyber Security Training

  Up until August 2023, the training was developed on a platform called 'Metacompliance'. The contract with Metacompliance ended in August 2023. The Council's Learning and Development Team has since developed the training and tailor made and designed to meet the specific needs of the Council.

  Although the training is available permanently via Sandwell Learn, the Governance Team run a campaign throughout May and June to launch the training and ensure the majority of staff complete the training during that period. This aligns to the requirement under the DSPT to train 95% of staff on an annual basis.

  The Governance Team also delivers in person training for those who are unable to access the training online.

  This training is also part of the induction process, thereby ensuring that new staff are trained early in their employment.

- FOI training

  This is delivered live by the Governance Team either via Teams or in person. Sessions are available to book onto via HR and are directed to those officers who deal with responding to requests under FOIA as part of their role.

- EIR training

  This is delivered live by the Governance Team either via Teams or in person. Sessions are available to book onto via HR and are directed to those officers who deal with responding to requests under EIR as part of their role.

- Processing Special Category Data Training

  This is delivered live by the Governance Team either via Teams or in person. Sessions are available to book onto via HR and are directed to those officers who process Special Category Data on a regular basis (eg ASC, Childrens)

15. Priorities for 2024-2025

The following priorities have been identified for 2024-2025

- Data Protection and Cyber Security training for members
- Finalise the implementation of the automatic email retention periods
- Agree and implement a work plan to meet the requirements of the Data Security and Protection (DSP) Toolkit 2024-2025
- Continued improvements with the Council's FOI compliance
- Continued improvements with the Council's SAR compliance
- Review of the use of 'Consent' as a lawful basis across the Council
- Develop a policy and guidance around the Council's use of AI
- Review of all Council contracts to ensure they are compliant with UK GDPR and Data Protection legislation.
- Develop guidance around bulk communications and use of BCC
- Cyber Assessment Framework
- Review of the Council's Multi Factor Authentication (MFA) and associated Privacy Notice
- Review of the Council's process for Bring Your Own Device (BYOD)
- Review of the use of fileshares across the council.