

TELFORD & WREKIN COUNCIL

AUDIT COMMITTEE 26 MAY 2022

INFORMATION GOVERNANCE & CALDICOTT GUARDIAN ANNUAL REPORT 2021/2022

JOINT REPORT OF THE AUDIT & GOVERNANCE LEAD MANAGER AND ADULT SOCIAL CARE DIRECTOR

1 PURPOSE

- 1.1 To present the 2021/2022 Information Governance (IG) & Caldicott Guardian Annual Report to the members of the Audit Committee.

2 RECOMMENDATIONS

- 2.1 That members of the Audit Committee note the Information Governance & Caldicott Guardian Annual Report for 2021/2022
- 2.2 That members of the Audit Committee agree the IG Work Programme for 2022/23

3 SUMMARY

- 3.1 The terms of reference of the Audit Committee include:
- *The Committee has the responsibility on behalf of the Council for the overseeing of the Council's audit, governance (including risk management) and financial processes*
 - *To be able to call senior officers and appropriate members to account for relevant issues within the remit of the Committee – governance (including information governance).*
 - *Consider the effectiveness of the Council's governance processes including The Council's information security framework*

4 PREVIOUS MINUTES

Audit Committee 14th July 2020 - Annual Internal Audit, IG and Caldicott Guardian Annual Report 2019/20

Audit Committee 27th May 2021 - Annual Internal Audit, IG and Caldicott Guardian Annual Report 2020/21

5 2021/2022 INFORMATION GOVERNANCE ANNUAL REPORT

- 5.1 There are a number of pieces of legislation and good practice standards that govern the IG arrangements of the Council and these are listed in the background information at the end of this report. The Information Commissioners Office (ICO) is the regulatory body responsible for ensuring Councils meet information legislative requirements relating to information governance.
- 5.2 The Local Authority Data Handling Guidelines recommend that each local authority should appoint a Senior Information Risk Owner (SIRO). The SIRO should be a representative at senior management level and has responsibility for ensuring that

management of information risks are weighed alongside the management of other risks facing the Council such as financial, legal and operational risk. At Telford & Wrekin Council the nominated SIRO for the period covered by this report was the Director: Policy & Governance.

Information Rights

5.3 Information rights is a collective name for 3 main pieces of legislation in respect to public sector information, these are:

- **Freedom of Information Act 2000** – encompasses any information held by the Council
- **Environmental Information Regulations 2004** – information with an environmental impact
- **UK Data Protection Act 2018/UK GDPR** – looks at personal information relating to individuals

5.4 The IG Team has continued to play a key role in providing assurance that the Council complies with information rights legislation during the year. The IG Team has responsibility for the administration of all information rights requests on behalf of the Council including the application of relevant exemptions in respect to requests received. It also co-ordinates and guides service areas when the Council receives a subject access request (someone requesting their personal information) or a request to access social care records, e.g. a parent asking to view the contents of their child's records.

5.5 The ICO has set a benchmark of 90% for responding to FOI requests within the 20 working day statutory deadline for responding to requests.

5.6 See table below for figures relating to FOI performance for the year 1 April 2021 to end of March 2022 compared with the same period for the previous year:

	20/21	21/22	% Increase / Decrease
Number of FOI requests received	1030	1031	0.1
Average number of FOI requests received per month	86	86	0
% of FOI requests responded to within statutory deadline	87	91	4
Average time taken (days) to respond to each request	12	14	1

As can be seen from the figures in the table above, the Council's performance in responding to FOI requests within statutory deadlines in 2021/22 increased by 4% comparable to the previous year.

In addition to the above the Council received 34 requests (37 in 20/21) that were processed under the Environmental Information Regulations (EIR) 2004. 88% (84% in 20/21) of these requests were responded to within the 20 day deadline.

5.7 In this period IG have received and responded to 37 appeals from requestors who were not satisfied with the response they received to their FOI request. This compares to a total of 28 appeals in 2020/21. To date only 8 of these appeals have been upheld/partly upheld.

- 5.8 During this period IG received 3 complaints/referrals from the Information Commissioner (ICO) in respect to complaints made to them in relation to freedom of information requests (2 complaints) and data protection requests (1 complaints).

The ICO did not take any action against the Council in relation to the complaints made to them. The ICO were satisfied that the Council had already complied with relevant legislation and/or provided further confirmation to the requesters in question.

- 5.9 The UK Data Protection Act 2018 requires the Council to respond to subject access requests (SARs) within one month of receipt unless the request is deemed complex when a further two month extension can be applied.

In 2021/22 the Council received 137 subject access requests, 6 less than the previous year.

Of the requests that had been responded to in 21/22, 88% were responded to within the legislative timescale set. This compares to 94% responded to within timescales in 20/21.

The processing of SAR's continues to be a challenge due to the volume (in pages) of information being asked for. 5 of the subject access requests received in 21/22 alone encompassed over 25,000 pages of information.

The IG Team continuously review their practices and look at the market for new technological solutions to ensure processes improve where possible.

Data Security Incidents

- 5.10 It is unrealistic to consider, given the amount of personal data Council services handle on a daily basis, that human errors will not occur which may result in a data breach. IG supports the investigation (with service areas) of all instances of alleged data breaches that are identified and referred to them. A data breach can cover a number of different incidents from a member/employee reporting a lost mobile phone to personal data being communicated to an unauthorised and/or incorrect recipient.

For each data breach identified in 2021/2022 a thorough investigation has been undertaken into how the breach occurred, confirmation of any individuals that have been informed in compliance with the Data Protection Act 2018 and lessons learnt identified and implemented to reduce the likelihood of similar data breaches occurring in the future.

The IG Team continues to work with service areas to improve the secure processing of personal data to prevent data security incidents.

- 5.11 The Council self-reported 1 data breach in 2021/22 as it met the criteria under the Data Protection Act 2018 for reporting to the Information Commissioners Office (ICO). In this instance the ICO were satisfied that the breach was due to human error and no further action was required.

Information Governance Related Audits & Work Programme

- 5.12 The 2021/2022 IG work programme was agreed at the May 21/22 Audit Committee. Progress to date in respect to this programme is shown attached as Appendix 1.

- 5.13 Appendix 2 details the proposed IG work programme for 2022/2023 for approval. This programme mainly incorporates key actions required to facilitate the legal requirements of the UK GDPR.

6 2020/2021 CALDICOTT GUARDIAN ANNUAL REPORT

Caldicott Guardian (CG) Function – Key Responsibilities

- 6.1 A requirement for the Audit Committee is to consider the Caldicott Guardians (CG) annual report / action plan. The first CG report was presented at the June 2015 Audit Committee meeting.

Caldicott Guardians were introduced into social care with effect from 1 April 2002, under Local Authority Circular LAC (2002)2 dated 31 January 2002. Caldicott Guardians play a key role in ensuring that the NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information under a framework which complies with the requirements of the Data Protection Act 2018; they actively support work to enable information sharing where it is appropriate to share; and advise on options for lawful and ethical processing of information

- 6.2 In February 2017 Sarah Dillon was appointed AD: Adult Social Care (now Director for Adult Social Care) and has since undertaken the role of Caldicott Guardian (CG).

- 6.3 In terms of CG activity please see summary below:

6.3.1 **GDPR** – the requirements of this legislation have been fully implemented with all staff completing relevant GDPR training. Each service continues to have an IG lead and receive and disseminate regular updates.

6.3.2 **Electronic Adult Social Care database and financial systems is well embedded and being updated to meet the requirements of the Care Reform legislation from 1/4/23** - The Data Protection Officer continues to support the service in monitoring the Data Protection Impact Assessment on the system. In 2020 there was a full audit of the financial management processes including the appropriate use of financial and case management systems and processes. The outcome of this audit provided assurance a further full audit is booked for 2023.

We are ensuring that the requirements of National Opt-out are complied with in the use of 'confidential patient information' as defined in section 251 (11) of the National Health Service Act 2006. Section 251's definition of patient has been expanded to include people who might more often be called service users/customers/clients and we are working to ensure projects are compliant and reviewing wider ASC use of confidential patient information accordingly.

The Adult Social Care electronic record self-service portal is still in development and will be implemented this year. This will mean that local people with care and support needs will be able to access some of their own care record and communicate directly with ASC via the portal. The system will enable online self-assessment including financial assessment which will enable us to implement the Care Reforms. The Data Protection Officer will be involved in completing the Data Protection Impact Assessment. This portal will mean that citizens with care and support needs will have an online account that they can access and use to manage their care and associated finances.

6.3.3 Adult Social Care Breaches – reporting system in place where IG inform the CG of all breaches related to social care data.

6.3.4 Integrated working with key partners – Information sharing protocols have been agreed and are updated regularly, supported by the Data Protection Officer. This will continue to be an important aspect as we further integrate service delivery and records with health partners as per the recent White Paper about the integration of health and social care and the development of our ICS (Integrated Care System) locally.

Our Telford and Wrekin Integrated Place Partnership (TWIPP) is our key local vehicle for development and delivery and a direct link to the ICS Board. There are work streams including Digital Information Governance Group which have regular input from the Caldicott Guardian and Data Protection Officer to ensure that all information governance requirements are met as we move towards further integrated pathways and partnerships.

The development of the Integrated Health and Care Record (One Health and Care) went live November 2021 for Adults and the Children’s Services version remains in development. The One Health and Care implementation has been a complex partnership programme and the Data Protection Officer has been central to this process with regular updates to the Caldicott Guardian and the TWC Senior Management Team. The Data Protection Officer attends the Integrated Care System Data Protection Group that monitors the compliance against the Data Protection Act, the group is attended by each organisation using One Health and Care. Communications with the public about the data protection aspect has been completed and the integration of health and care records is already showing improved communications between professionals and improved outcomes for the citizen. There is an internal audit planned in July 22 around the implementation of One Health and Care.

There is a new ICS Caldicott Guardian Group being convened which the TWC Caldicott Guardian will attend to ensure join up and continual development of practice.

6.3.5 Quality Assurance – Regular review meetings are in place with the Senior Information Risk Owner, CG and Data Protection Officer to ensure that further development and assurance of our data protection systems continue in relation to our support of those with care and support needs particularly as we integrate records and delivery further with health and care partners.

7 CONCLUSIONS FOR 2021/2022

- 7.1 The Information Governance Team have performed well and made a positive contribution to the governance arrangements within the Council in 2021/2022.

8 OTHER CONSIDERATIONS

AREA	COMMENTS
Equal Opportunities	All members of the IG Team have attended equal opportunities/ diversity training. If any such issues arose during any work the appropriate manager would be notified.
Environmental Impact	All members of the IG Team are environmentally aware and if any issues were identified they would be notified to the appropriate manager.
Legal Implications	Compliance with the Information Rights legislation mentioned in this report is mandatory. When assessing compliance, the ICO will consider approved policies and procedures of the authority.

	<p>NHS and Social Care Caldicott Guardians are required to be registered on the publicly available National Register of Caldicott Guardians. The UK Council of Caldicott Guardians, an elected body made up of Caldicott Guardians from health and social care, meets four times per year and publishes a manual for Caldicott Guardians (currently 2017) which sets out the roles and responsibilities of the Caldicott Guardian. The Health & Social Care Information Centre [HSCIC] publishes guidance and resources for Caldicott Guardians.</p> <p>RP 5/5/22</p>
Links with Corporate Priorities	All aspects of the IG teams work support good governance which underpins the achievement of the Council's objectives and priorities.
Risks and Opportunities	All aspects of the IG teams work supports managers and the Council to identify and manage their information risks and opportunities.
Financial Implications	Costs associated with the Information Governance and Caldicott Guardian work outlined in this report are met from the Council's base budget. AEM 28.04.22
Ward Implications	The work of the IG team encompasses all the Council's activities across the Borough and therefore it operates within all Council Wards.

9 **BACKGROUND PAPERS**

Corporate Information Security Policy

Corporate Information Security Breach Procedure

Local Authority Data Handling guidelines

ISO27001 (standard for information security)

Data Protection Act 2018

Freedom of Information Act 2000 (fully introduced 2005)

Environmental Information Regulations 2004.

Caldicott Review - <https://www.gov.uk/government/publications/the-information-governance-review>

Information: To Share or not to Share – Government Response to the Caldicott Review.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Report by Rob Montgomery Audit & Governance Lead Manager. Telephone 383103

Update on Information Governance (IG) Work/Compliance Programme 2020/2021

No	Task	Completion Date	Update as at 31/3/21
1	Administer FOI/EIR/DPA requests, appeals and associated correspondence from the ICO.	Ongoing	Performance comparable with 2021/22
2	Continue the provision and promotion of additional services to schools within and outside the area to generate agreed income.	Ongoing	IG Team continues to provide services for a number of parish councils, schools and academy trusts.
3	Investigate instances of possible data breaches and ensure appropriate improvements within services and processes are made.	Ongoing	Ongoing support to services and liaison where necessary with ICO.
4	Support service areas to address any information security risks that arise.	Ongoing	As above.
5	Monitor compliance with GDPR/DPA 2018 and associated Council policies. This includes the assignment of responsibilities, awareness raising, training of staff and associated audits.	Ongoing	Compliance work completed in year contributing to accountability principle.
6	To provide advice where requested on Data Protection Impact Assessments (DPIA) and monitor performance in this area.	Ongoing	DPIA's completed on a number of projects in year that are reviewed and signed off by IG.
7	To co-operate with the Information Commissioners Office (ICO) in any relevant engagement.	Ongoing	The IG Team continue to be the key contact with ICO.
8	Inform and advise the Council and its employees who carry out personal information processing of their obligations under GDPR/DPA 2018.	Ongoing	The IG Team provides various updates to staff throughout the year.
9	Review and update the Corporate Information Security Policy (CISP)	End of March 2022	Policy currently under review – due for completion by end of May 2022.
10	Complete Data Security & Protection (DSP) toolkit assessment for central government.	End of July 2022	Complete.

Information Governance (IG) Work/Compliance Programme 2022/2023

No	Task	Completion date
1	Administer FOI/EIR/DPA requests, appeals and associated correspondence from the ICO.	Ongoing
2	Continue the provision and promotion of additional services to schools within and outside the area to generate agreed income.	Ongoing
3	Investigate instances of possible data breaches and ensure appropriate improvements within services and processes are made. This would include acting as a point of contact for the ICO.	Ongoing
4	Support service areas to address any information security risks that arise. This would include acting as a point of contact for the ICO.	Ongoing
5	Monitor compliance with GDPR/DPA 2018 and associated Council policies. This includes the assignment of responsibilities, awareness raising, training of staff and associated audits.	Ongoing
6	To provide advice where requested on Data Protection Impact Assessments (DPIA) and monitor performance in this area.	Ongoing
7	To co-operate with the Information Commissioners Office (ICO) in any relevant engagement.	Ongoing
8	Inform and advise the Council and its employees who carry out personal information processing of their obligations under GDPR/DPA 2018.	Ongoing
9	Review and update the Corporate Information Security Policy (CISP).	End of March 2023
10	Complete Data Security & Protection (DSP) toolkit assessment for central government.	End of July 2023