TELFORD & WREKIN COUNCIL

AUDIT COMMITTEE 30 MAY 2019

INFORMATION GOVERNANCE & CALDICOTT GUARDIAN ANNUAL REPORT 2018/19

JOINT REPORT OF THE AUDIT & GOVERNANCE TEAM LEADER AND ASSISTANT DIRECTOR ADULT SOCIAL CARE

1 PURPOSE

1.1 To present the 2018/19 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 2018/19

2.2 That members of the Audit Committee agree the IG Work Programme for 2019/20

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 27th June 2017 - Annual Internal Audit, IG and Caldicott Guardian Annual Report 2016/17

Audit Committee 29th May 2018 – Annual Internal Audit, IG and Caldicott Guardian Annual Report 2017/18

5 2018/19 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 Council's meet information legislative requirements.

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 Assistant Director: Governance, Procurement & Commissioning.

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
- **Data Protection Act 2018** – 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 2018 to end of March 2019 compared with the same period for the previous year:

	17/18	18/19	% Increase / Decrease
Number of FOI requests received	1064	1155	9
Average number of FOI requests received per month	89	96	8
% of FOI requests responded to within statutory deadline	80	81	1
Average time taken (days) to respond to each request	14	14	0

As can be seen from the figures in the table above, the Council's performance in responding to FOI requests within statutory deadlines improved slightly (up by 1%) from 2017/18.

In addition to the above the Council received 34 requests (29 in 17/18) that were processed under the Environmental Information Regulations (EIR) 2004. 79% (86% in 17/18) of these requests were responded to within the 20 day deadline.

5.7 In this period IG have received and responded to 16 appeals from requestors who were not satisfied with the response they received to their FOI request. This compares to a total of 11 appeals in 2017/18.

5.8 During this period IG received 2 complaints/referrals from the Information Commissioner (ICO) in respect to complaints made to them by FOI/EIR requestors. The first complaint

was due to an FOI request not responded to within 20 working days which the Council subsequently responded to. The second complaint was made where the requester did not agree with the FOI exemptions applied by the Council to their request. The ICO partially decided in favour of the Council.

5.9 The introduction of the General Data Protection Regulations changed the response times for responding to a Subject Access Request. Therefore for 2018/19 the following legislative response times were in place:

- 1/4/18 – 25/5/18 Legislative response rate 40 calendar days
- 26/5/18 – 31/3/19 Legislative response rate of 1 calendar month (with the option of extending for a further 2 months for complex requests)

Therefore between 1 April 2018 and 25 May 2018 the Council received 6 Subject Access Requests (SAR's). The Council responded to 4 SAR's within the 40 calendar day deadline.

Between 26 May 2018 to 31 March 2019 the Council received 85 Subject Access Requests (SAR's). The Council responded to 56 SAR's within either 1 calendar month and/or the extension of a further 2 months for complex requests.

Therefore the number of SAR requests in 2018/19 have nearly doubled from the number received in the previous year.

It should be noted that the size and complexity of subject access requests increases year on year. For 91 requests responded to in 2018/19, the IG Team had to read and redact over 13,000 pages of mainly sensitive personal social care information. IG continually review its procedures for processing subject access requests and feel that these are streamlined and fit for purpose. However further reviews will take place 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 2018/19 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 2 data breaches in 2018/19 as these met the criteria under the Data Protection Act 2018 for reporting to the Information Commissioners Office (ICO). In both cases the ICO were satisfied that breaches were due to human error and no further action was required in either case. In addition the ICO received a referral directly from an individual alleging that a data breach had been caused by the Council. After investigating

this matter the ICO decided that there was no evidence to suggest a breach had occurred.

Information Governance Related Audits & Work Programme

5.12 The 2018/19 IG work programme was agreed at the May 2018 Audit Committee. Progress to date in respect to this programme is shown attached as Appendix 1.

5.13 The implementation of the General Data Protection Regulations (GDPR) across the Council was audited by TIAA (an external audit company) as part of the contract for TIAA to provide IT audit services to the Council. The outcome of the audit was that there was reasonable assurance (Yellow report) that the Council were complying with GDPR requirements. Three recommendations (none high risk) have been made which have been taken on board by the IG Team and associated action plans for implementation agreed with TIAA. This was a pleasing outcome given the complexity of GDPR requirements.

5.14 Appendix 2 details the proposed IG work programme for 2019/20 for approval. This programme mainly incorporates key actions required to facilitate the legal requirements of the GDPR.

6 2018/19 CALDICOTT GUARDIAN ANNUAL REPORT

Caldicott Guardian (CG) Function – Key Responsibilities

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

6.2 In February 2017 Sarah Dillon was appointed AD: 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 **New electronic Adult Social Care database and financial systems** – In October 2018 the new system went live. The Data Protection Officer supported the service in completing a Data Protection Impact Assessment on the system. In 2020 the new system is to be audited.

6.3.3 **Adult Social Care Breaches** – new 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, supported by the Data Protection Officer. This will continue to be an important aspect as we further integrate service delivery with partners as per the requirements of the NHS Plan. A part of this is the further development of the Sustainability and Transformation Plan across the health and social care system and the development of the Integrated Care System and an Integrated Telford Place Based Board. There are work streams including Digital Information Governance Group which will require 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.

6.3.5 **Quality Assurance** – Regular review meetings are planned with the Senior Information Risk Owner, CG and Data Protection Officer over the next 12 months 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.

7 CONCLUSIONS FOR 2018/19

7.1 Despite limited resources and significant staff absence the Information Governance Team have performed well and made a positive contribution to the governance arrangements within the Council in 2018/19.

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. Each NHS organisation is required to have a Caldicott Guardian under Health Service Circular HSC 1999/012 dated 22 January 1999. The Circular applies to all organisations which have access to patient records, including acute trusts, ambulance trusts, mental health trusts, primary care trusts, strategic health authorities, and special health authorities such as NHS Direct. Caldicott Guardians were subsequently 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 1998; 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. 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 has a published strategy, currently for 2011-2016. The Health & Social Care Information Centre [HSCIC] publishes guidance and resources for Caldicott Guardians. SD 19.04.2017
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	The work required to implement the 2019/20 IG plan will be met from within existing resources. There are therefore no financial implications arising from adopting the recommendations of this report.
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 Team Leader. Telephone 383103

APPENDIX 1

Update on Information Governance (IG) Work/Compliance Programme 2018/19

No	Task	Completion Date	Update as at 31/3/19
1	Administer FOI/EIR/DPA requests, appeals and associated correspondence from the ICO.	Ongoing	Complete
2	Continue the provision and promotion of additional services to schools within and outside the area to generate agreed income.	Ongoing	Complete
3	Investigate instances of possible data breaches and ensure appropriate improvements within services and processes are made.	Ongoing	Complete
4	Support service areas to address any information security risks that arise.	Ongoing	Complete
5	Support information sharing/production of sharing agreements.	Ongoing	Complete
6	Support service areas in the completion of Data Protection Impact Assessments for new systems/applications and those for priority existing applications.	Ongoing	Complete
7	GDPR Compliance	Ongoing	Complete
8	Review of IG training and awareness	October 2018	Complete
9	Review and update the Corporate Information Security Policy (CISP)	End of March 2019	Complete
10	Complete N3 connection assessment for central government.	End of March 2019	Complete

APPENDIX 2

Information Governance (IG) Work/Compliance Programme 2019/20

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.	End of June 2019
9	Implementation of the GDPR audit recommendations.	End of July 2019
10	Review and update the Corporate Information Security Policy (CISP).	End of September 2019
11	Complete Data Security & Protection (DSP) toolkit assessment for central government.	End of March 2020