



REPORT TO AUDIT AND RISK ASSURANCE COMMITTEE



21 March 2019

| | |
|--|---|
| Subject: | Update on Information Governance Compliance |
| Director: ■ | Surjit Tour Director - Law and Governance and Monitoring Officer |
| Contribution towards Vision 2030: ■ |   |
| Contact Officer(s): | Philip Tart - Interim Monitoring Officer Daniel Okonofua – GDPR Consultant |

DECISION RECOMMENDATIONS

That Audit and Risk Assurance Committee

Notes the update provided in relation to the Council's position on Information Governance compliance, pursuant to the General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA) and the NHS Toolkit.

1 PURPOSE OF THE REPORT

- 1.1 To provide an update on the Council's implementation of the General Data Protection Regulation (GDPR), now incorporated within Data Protection Act 2018 (DPA), and the National Health Service's (NHS) Data Security and Protection Toolkit (DSPT).

2 IMPLICATIONS FOR VISION 2030

- 2.1 Providing protection and responsible stewardship of personal information on behalf of our communities will support the achievement of Ambition 5 – ensuring our communities feel safe and protected.
- 2.2 Setting the standard for Data Protection regulatory compliance will give the council a trusted name and positive reputation among Local

Authorities nationwide, thus supporting the realisation of Ambition 10 - national reputation for getting things done.

3 **BACKGROUND AND MAIN CONSIDERATIONS**

3.1 The Data Protection Act 2018, incorporating the GDPR, came into effect on May 25, 2018.

3.2 The GDPR builds on existing legislation to achieve the following objectives:

- Updates the law on information governance to take account of advancements in science and technology
- Ensure consistency in the processing of personal information across EU member states
- Enhances the rights of individuals over the collection, use, sharing and storage of their personal data.

3.3 The Information Commissioner's Office has made it clear that organisations must have a plan in place to ensure compliance with the DPA 2018. On May 23, 2018, the ICO issued a press statement confirming May 25, 2018 as the GDPR go live date in the UK and stated:

“The creation of the Data Protection Act 2018 is not an end point, it's just the beginning, in the same way that preparations for the GDPR don't end on 25 May 2018. From this date, we'll be enforcing the GDPR and the new Act but we all know that effective data protection requires clear evidence of commitment and ongoing effort.

It's an evolutionary process for organisations – no business, industry sector or technology stands still. Organisations must continue to identify and address emerging privacy and security risks in the weeks, months and years beyond 2018.

As long as there is data protection law the ICO is here to help. We have a whole host of guidance and resources on our website and we'll keep doing the same job we've always done, offering advice, guidance and education for everyone who needs it”

3.4 The Council has implemented a number of actions and introduced measures that demonstrate proactive steps towards full DPA 2018 compliance. There is also a plan in place to enable all outstanding actions to be completed in a timely manner so that the Council will be compliant with both the NHS Toolkit (by 31 March 2019) and the DPA 2018 (by 31 March 2020).

- 3.5 The NHS Data Security and Protection Toolkit is an online self-assessment tool that all organisations must use if they have access to NHS patient data and systems. Given the council's need to access NHS data and systems for the effective delivery of children's services and adult services, the council's compliance with this toolkit is therefore compulsory.
- 3.6 The Council has for the last 18 months had an Information Governance Board (IGB), chaired by the Senior Information Risk Owner (SIRO) (who is the Council's Director of Law and Governance and Monitoring Officer). The SIRO oversees Information Governance within the Council and monitors compliance activity.
- 3.7 As at 25 May 2018, the council undertook many actions such as introducing the new one month response time for subject access requests, negotiating and entering into data sharing agreements, record of processing activities documentation and introduction of a data protection impact assessment for new systems and information capturing processes.
- 3.8 The Council is able to demonstrate that it has met the expectation of the Information Commissioner as outlined in paragraph 3.3 above as at 25 May 2018. Since that date the Council has continued to progress its Information Governance action plan – further details of which are set out below.

4 THE CURRENT POSITION

- 4.1 The SIRO commissioned a diagnostic exercise of the work undertaken by the Council in relation to the DPA 2018 and NHS toolkit, following national developments post May 2018 and changes in staff.
- 4.2 The outcome of this diagnostic process has resulted in a four-phased action plan being developed, that monitors and manages all Information Governance activities from November 2018 through to March 2020. (**See Appendix A**).
- 4.3 Delivery of the NHS toolkit for the 2018/2019 and 2019/2020 financial years is incorporated into the action plan.
- 4.4 Phase one of this plan was completed in February 2019 and the Council is on course to ensure full compliance with the NHS Toolkit by 31 March 2019 as required.

- 4.5 The action plan has been structured around the ICO's 'Steps to Compliance' which consists of ten work streams, broken down into seventy specific tasks (**See Appendix B**). These seventy tasks are captured within the action plan.
- 4.6 Currently, phase one of this plan has been completed accounting for nineteen tasks and 27% of remedial activity (**See Appendix C**). The Council has also completed 52% of the activity for NHS toolkit compliance due for submission at the end of March 2019. The remainder whilst sizeable in percentage terms, the actual activity associated with the remaining 48% are the evidence required for the Council's Information Asset Register, evidence required for sufficient third party sharing agreements, evidence required of data protection training for a minimum 95% of employees and the Council's public sector network certification. All of these are well in hand and verging on completion.
- 4.7 The Information Governance Board was refreshed in December 2018 (**See Appendix D**). The new Board membership consists of the SIRO, the Data Protection Officer (DPO), the Caldicott Guardian, Head of ICT and representatives from Audit, Risk and Insurance, Human Resource, Adult Social Care Health and Wellbeing (ASCHW), Neighbourhoods, Education, Finance, Law and Governance.
- 4.8 The IGB provides operational oversight of all Information Governance activity and will ensure the action plan is delivered in a timely manner.

Elected Members

- 4.9 The Action Plan acknowledges the role of Elected Members as Data Controllers and it is essential that Elected Members also understand their Information Governance obligations.
- 4.10 The 2002 statutory instrument on data protection for Elected Members, confers on them the authority to act on a request made by a data subject. This authority also places the responsibility of a data controller on Elected Members.
- 4.11 The DPA 2018 has not had significant changes upon Elected Members. However, it has provided an opportunity for obligations to be clarified and ensure Elected Members understand their obligations, duties and responsibilities in relation to Information Governance.
- 4.12 Members need to have effective systems in place to:
- Receive, manage, store, share and destroy personal information that they receive as part of their role.
 - Understand their obligations in relation to sensitive personal information (such as a resident's medical information) - namely

that they need express, written consent to collect or share such information for the purposes it has been provided.

- Manage information given in confidence or confidentially.

4.13 The Local Government Association has issued guidance to Elected Members, and that guidance has been shared with all Members of the Council.

4.14 Specific training for Elected Members is being devised for June and July 2019. The training will cover:

- Induction training for newly elected members (if any)
- Overview of legal duties, obligations and responsibilities
- Scenarios based training
- Managing information effectively
- Individual data protection advice tailored to members (if required)

4.15 The training will be delivered through the Member Development Programme.

5 CONSULTATION (CUSTOMERS AND OTHER STAKEHOLDERS)

5.1 There is no formal consultation obligation arising from this report save that every effort will be made to ensure the needs of Elected Members are captured and addressed.

6 ALTERNATIVE OPTIONS

6.1 The Council must ensure compliance with the DPA 2018 and NHS Toolkit.

6.2 The SIRO will adapt the approach and methodology in delivering Information Governance compliance as necessary to ensure the Council meets its legal obligations in this area.

7 STRATEGIC RESOURCE IMPLICATIONS

7.1 The Council has secured additional professional support to help implement the action plan.

7.2 The Director of Law and Governance & Monitoring Officer has also restructured his directorate and established a Governance and Business Support Team with increased resources to ensure the Council has the

capability, skill-sets and ability to implement the action plan and drive continuous improvement in this area of practice.

8 LEGAL AND GOVERNANCE CONSIDERATIONS

8.1 These implications have been set out in the main body of the report.

9 EQUALITY IMPACT ASSESSMENT

9.1 All relevant action will be subject to an appropriate equalities assessment to ensure all requisite needs of Elected Members, staff and relevant persons are addressed.

10 DATA PROTECTION IMPACT ASSESSMENT

10.1 No Data Protection Impact Assessment is required in respect of this report.

11 CRIME AND DISORDER AND RISK ASSESSMENT

11.1 There are no crime and disorder risks arising from this report.

12 SUSTAINABILITY OF PROPOSALS

12.1 There are no direct sustainability issues arising from this report.

13 HEALTH AND WELLBEING IMPLICATIONS (INCLUDING SOCIAL VALUE)

13.1 There are no direct health and wellbeing implications from this report.

14 IMPACT ON ANY COUNCIL MANAGED PROPERTY OR LAND

14.1 There is no direct impact on any council managed property or land from this report.

15 CONCLUSIONS AND SUMMARY OF REASONS FOR THE RECOMMENDATIONS

15.1 The purpose of this report is to update the Audit and Risk Assurance Committee with regards the Council's compliance with the DPA 2018 and NHS Toolkit.

16 BACKGROUND PAPERS

16.1 None

17 **Appendices**

Appendix A - 4 Phase Action Plan

Appendix B - ICO 'Steps to Compliance'

Appendix C - Status of the 70 tasks in the 4 Phase Action Plan

Appendix D - The Information Governance Board and Membership

GDPR/DPA Phased Remediation Plan



NOVEMBER 2018 – FEBRUARY 2019

phase 1

S
t
a
r
t

- GDPR/DPA gap analysis
- Remediation Action Plan
- Reconstitution of Information Governance Board
- Privacy Notice draft, design and roll out
- Mandatory Data Protection and Cyber Security training design and roll out



FEBRUARY 2019 – MARCH 2019

phase 2

- NHS toolkit evidence collation and submission
- Information Asset Register roll out
- Third party organisations contract tracker
- Start of intranet and website content review



APRIL 2019 – JUNE 2019

phase 3

- Information Governance policy review
- Cabinet Members training and support
- Information Asset Register audit
- Launch of DPO traded service for schools
- Restructure of Information Management Unit



GDPR/DPA Phased Remediation Plan

JULY 2019 – DECEMBER 2019

phase 3

- Mandatory training design x2 modules
- NHS toolkit evidence collation
- Records management audit
- Training for new Information Management staff



GDPR/DPA Phased Remediation Plan



ICO's Steps to Compliance



Awareness

- Establishment of a central forum with the appropriate level of authority to govern information
- Council wide understanding of responsibility for information governance oversight
- Timely and adequate level of management briefing for EMT and Cabinet Members
- The presence of a regularly updated corporate risk register updated with information management risks.
- An emergency communication plan



ICO's Steps to Compliance

Information you hold

- Up to date record of all information assets
- Information asset record captures record of processing activities
- Disaster recovery plan
- Comprehensive record retention schedule
- Established process of information asset review
- Record disposal procedure is documented, audited and reviewed at established intervals



Communicating privacy information



- Privacy Notices have been updated and conform with GDPR requirements
- Intranet guidance for employees has been updated
- Data Subjects have access to information that educates them of their personal information rights
- System functionality can accommodate the rights of individuals under the law

Individual's rights



ICO's Steps to Compliance

Subject access requests



- Policy guidance and process updates to include the one month statutory requirement for response to Subject Access Requests
- Review of the Council's resource capability to accommodate the changes

Lawful basis



- Lawful basis for processing information is included with record of processing activities against every information asset



ICO's Steps to Compliance



Consent



- A review of all forms where consent is the lawful basis for collecting information
- Assurance that system capability can manage consent as prescribed in the regulation

Children



- A complete review of all policy, people, processes and technology capturing childrens information



Data breaches

- Updated policy and guidance for identification, reporting and management of Data Breaches
- Review of resource capability to comply with the statutory 72 hour requirement to report serious incidents to the ICO
- Ensure the Council has adequate Insurance policy against Data Breach indemnity



ICO's Steps to Compliance

Data Protection by Design & DPIA

- Embed a functional Data Protection Impact Assessment process into all information asset procurement activity
- Evidence that all responsibility for the creation and maintenance of information assets rests with identified individuals
- Establishment of a system of review for cyber security adequacy
- Administration of relevant and effective data protection and cyber security training across the Council annually
- Review of the Council's information governance structure to satisfy transparency requirement and minimise conflict of interest



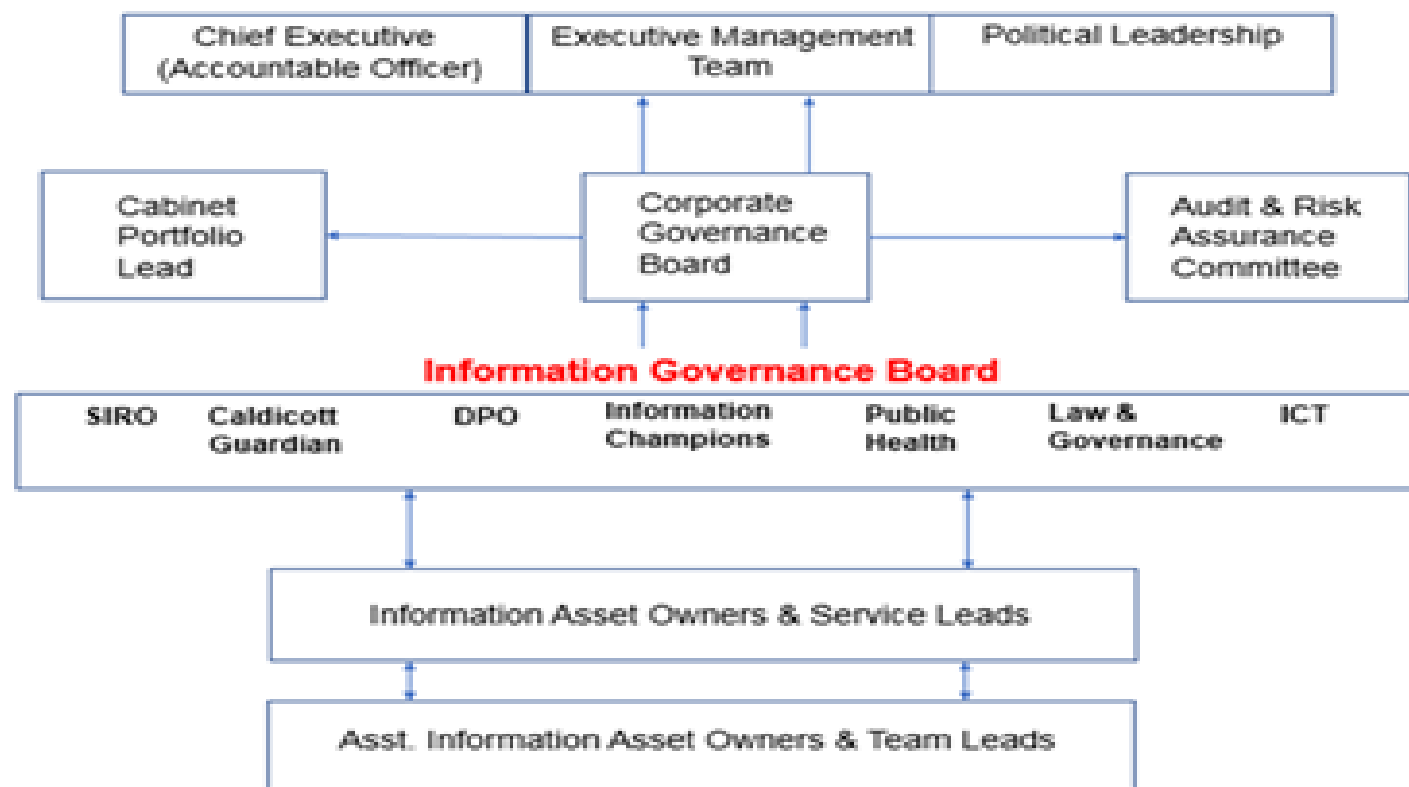
ICO's Steps Task Status

| ICO Steps | Total Tasks | Complete Tasks | WIP Tasks | Not Started |
|---|-------------|----------------|-----------|-------------|
| Awareness | 8 | 5 | 1 | 2 |
| Information You Hold | 9 | 0 | 6 | 3 |
| Communicating Privacy Information | 4 | 2 | 1 | 1 |
| Individual Rights | 2 | 1 | 0 | 1 |
| Subject Access Requests | 4 | 0 | 3 | 1 |
| Lawful Basis | 4 | 0 | 4 | 0 |
| Consent | 3 | 0 | 0 | 3 |
| Children | 2 | 0 | 1 | 1 |
| Data Breaches | 5 | 0 | 2 | 3 |
| Data Protection by Design and Data Protection Impact Assessment | 29 | 11 | 8 | 10 |
| Total | 70 | 19 | 26 | 25 |





IG Board Reporting Structure



IGB Membership



SIRO

Caldicott Guardian

DPO

Head of ICT

IC's for HR & Law and Governance

IC's for ASC & Public Health

IC's for Finance & Audit/Risk

IC's for Children's & Neighbourhoods

Chair

Alternative Chair

Alternative Chair

Member

Member

Member

Member

Member

