WIRRAL

AUDIT AND RISK MANAGEMENT COMMITTEE 9TH MARCH 2021

REPORT TITLE:	**INFORMATION GOVERNANCE UPDATE**
REPORT OF:	**DIRECTOR OF LAW AND GOVERNANCE**

REPORT SUMMARY

This report provides an update on the work being done to sustain and deliver effective Information Management relating to Information Governance across the Council, reducing the risk of reputational damage and monetary penalties. It also highlights areas of Information Governance work in the coming year.

This matter affects all Wards within the Borough. It is not a key decision.

RECOMMENDATION

The Audit and Risk Management Committee are recommended to note the report.

SUPPORTING INFORMATION

1.0 REASON/S FOR RECOMMENDATION/S

1.1 To enable the committee to understand the Authority's current position regarding Information Management in relation to Information Governance and any significant risks. It also outlines the current controls in place and frameworks, to ensure the Authority can have confidence in its Information Governance arrangements.

2.0 OTHER OPTIONS CONSIDERED

2.1 The report is for information purposes and as such no other options considered.

3.0 BACKGROUND INFORMATION

3.1 The Council's information governance arrangements were reviewed in advance of the General Data Protection Regulation (GDPR) which came fully into force in May 2018. GDPR was the first real change to data protection legislation in the past 20 years and this also led to the Data Protection Act 2018 being enacted. This legislation strengthened the rights of individuals in relation to how their personal data was collected, stored, used, shared, kept secure and destroyed.

3.2 The Council was required to appoint a statutory Data Protection Officer (DPO) who acts independently of the Council to provide effective Data Protection advice and guidance to Officers, the public and elected members.

3.3 A full review of Information Governance policies and procedures was required to ensure they were transparent and compliant with the new legislation; the Council's websites also required a full review to ensure compliance.

3.4 Additional support for the Data Protection Officer was put in place by the Law and Governance department in 2017 by funding a GDPR Officer for a 12 month period.

3.5 Current support for the Data Protection Officer remains in place by Law and Governance department specifically making legal time available each week for complex Information Governance Issues. The Senior Information Risk Officer (SIRO) also provides support and oversight, the current SIRO is Director of Law and Governance.

3.6 As the landscape has changed over the past 12 months with the advent of Covid-19 meaning approximately 2,000 employees are working from home; this has altered the Information Governance risks and the mitigation required to minimise those risks.

3.7 The body of this report details some of the work undertaken in the past 12 months to help mitigate the changing risks in relation to Information Governance. It also sets out a plan for the next 12 months which will help to ensure the Council's compliance in a number of information management and data protection policy areas.

Information Governance Risks

3.8 Following the review of Information Governance and Data Protection arrangements it was established that two key risks warranted inclusion on the Corporate Risk Register. These are:

- CRR23 - Cyber Security, the risk description states that “IT security is insufficient to deter, detect and prevent unauthorised access to IT systems, resulting in loss of data and disruption to Council Services”.
- CRR24 - Information Management which states that “Failure of the Council to comply with relevant data and information management legislation which may lead to loss or breach of personal data creating security or reputational damage”.

3.9 The Information Governance Board (IGB), chaired by the DPO, meets regularly and manages and monitors its own subject specific risk register of information management risks across the Council.

3.10 The IGB Risk Register currently contains 10 risks including those relating to records management; both corporate systems and the potential amount of unlisted and unmanaged information / records in both paper and electronic form, a lack of awareness and understanding of information management and information/cyber security responsibilities across Council, a failure to maintain policies and procedures for records management, information security and information management to reflect current working practices. The work undertaken and planned for 2020/2021/2022 will help mitigate and manage the risks.

IG Work in 2020/21

3.11 Due to the massive impact of Covid-19 and the need to move sensitive personal information between the Council and partner agencies such as NHS and Public Health England, an enormous amount of work was generated to be overseen by the DPO. This included the requirement for privacy notices to be drawn up to reflect and demonstrate new purposes why the Council needed to process data. Privacy notices help the Council demonstrate transparency on how and why they use people’s personal data.

3.12 In addition a large number of Data Sharing agreements were required to be drawn up and reviewed and agreed. For example, charitable organisations such as Barnardo’s engaged with the Council to help vulnerable families and robust data sharing arrangements were key. The Council DPO also acts as Data Protection Officer for many schools and was called upon to give advice and guidance to them in relation to sharing information for families who required food hampers in the school holidays.

3.13 The impact of COVID-19 has been felt in many ways across the various teams. Some areas have seen a dramatic increase in work, such as the Records Management Team. The following information and statistics help to demonstrate the variety and scale of the work involved.

Statistical snapshot of Information Governance work

Security Incidents

3.13.1 The table below provides a breakdown of the reported security incidents in the past two years. The incident severity categorisation is assessed by the Information Security Team.

Incident Severity Assessment	**2019/20**	**2020/21 – up to January 21**
Severe	11	7
Moderate	23	33
Low	93	77
Informational	10	4
Undetermined	0	2
Total	**137**	**123**

All incidents are discussed in a fortnightly meeting and severe cases will be escalated through to the relevant service manager for appropriate actions to be taken. This may include changes to processes or refreshing staff training.
In 2019/20 there were 7 incidents reported to the Information Commissioner Office (ICO) and to date 2020/21 there have been 4. Some incidents reported are independent of the table above as individuals may go directly to the ICO if they have a complaint.

Requests for Information

3.13.2 Freedom of Information (FOI); Environmental Information Regulations (EIR) and Subject Access Requests (SARS) are subject to legally prescribed timescales within which the Council must respond. They have been reported corporately on an as "closed in month" basis for several years. Total FOI/EIR requests in 2018/19 were 1752 with SARs totally 214 in that year. Numbers received have dropped slightly since the start of the pandemic. The table below gives figures for the past two years.

Closed in Month	**19/20 FOI/EIR**	**20/21 FOI/EIR**	**19/20 SAR**	**20/21 SAR**
April	141	59	15	3
May	151	84	11	6
June	141	81	18	9
July	156	72	28	17
August	145	106	19	16
September	126	106	31	16
October	128	128	20	6
November	139	129	12	7
December	94	89	9	8
January	149		14	
February	148		15	
March	100		8	

Totals	**1618**	**854 to Dec 20**	**212**	**88 to Dec 20**

Archives Service Statistics

3.13.3 Visitor numbers to the Archives Search room at Cheshire Lines Building between April 2019 to early March 2020 totalled 768. There have been no visitors since the March 2020 lockdown due to COVID restrictions. Archival enquiries have continued to be answered as remote enquiries throughout Covid

- Apr 2019 to Mar 2020 – 272 enquiries
- Apr 2020 to 10 Feb 2021 (Year to date) – 262 enquiries

Records Management Statistics

3.13.4 Transfers in of records - Since COVID, Records Management has played a key role supporting Asset Consolidation Staff Relocation (ACSR) and clearing buildings of records. This is reflected in the amount of material transferred into the records management facility. Normal transfer figures are 70 boxes a month, with 716 received in 2019/20. However, to support ACSR, 1,400 boxes were received in the eight months between Apr 2020 and Nov 2020, averaging over 180 boxes a month. A further 433 were received in December and January.

Appraisals of records

3.13.5 ACSR has involved not only mass transfer of records but also the appraisal (in relation to informational or archival value) of a large number of records left in buildings. This is very time consuming and has constituted a very large proportion of the team's workload over the last year. Arrowe Hill material, in the Conway Building, alone numbered 1,200 boxes A further 1,000 boxes have come from the North Annexe (Planning etc.) and Cheshire Lines.

Future plans

3.14 The additional demands of the COVID-19 response have led to some activities being delayed. However, several key activities to assist in mitigating and managing the risks mentioned above are planned or already underway in relation to Information Management. Key actions include:

- New e-learning courses are available to staff to ensure they are aware of their responsibilities when handling data
- Additional staffing resources are being made available to work with the Data Protection Officer
- Continuous review of Information Management policies and procedures to ensure they adequately cover the changes to agile working
- Use of communication channels for staff awareness messages to remind them of the responsibilities everyone has.

3.15 With regard to mitigating and managing risks in relation to Cyber Security the following activities are planned or already in progress:

- New e-learning essential training courses available to all staff to ensure they are aware of how to stay safe online. Currently at 9th February 202, 682 have already completed this essential training.
- Use of CXO Brief and Managers Brief to communicate about Cyber Security.
- Creation of a Cyber Security Board and new Cyber Security Policy being drawn up. Council seeking Cyber Essentials accreditation which is a government backed scheme which helps you to protect your organisation.

3.16 With regard to compliance with Data Security and Protection Toolkit (DSPT), this is an annual self-assessment for health and care organisations. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly. Failure to comply with the DSPT requirements could impact on our access to NHS patient data. From 2021/22 the self-assessment process and compliance requirements will be owned by Health and Social Care with advice and support to complete the toolkit available from key officers within ICT. The Council is currently compliant with DSPT.

3.17 With regard to compliance with The Payment Card Industry Data Security Standard (PCI DSS), this is an information security standard for organisations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. There are over a dozen business areas across the Council who need to maintain PCI DSS compliance including leisure and car parking facilities. A Project Officer has been allocated from the business change team to review work to date and then produce a project plan to ensure full compliance by end of 2021.

4.0 FINANCIAL IMPLICATIONS

4.1 There are no immediate financial implications arising directly from this report.

5.0 LEGAL IMPLICATIONS

5.1 Public Bodies have a statutory duty to appoint a Data Protection Officer who is required to assist in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO). This Officer must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

5.2 The Data Protection Officer has responsibility for advising on and agreeing Data Sharing Agreements and Privacy Notices which demonstrate our transparency when processing information. They also have a key role in ensuring the Council is complaint with current and emerging information governance requirements.

6.0 RESOURCE IMPLICATIONS: STAFFING, ICT AND ASSETS

6.1 There are no resource implications arising directly from this report.

7.0 RELEVANT RISKS

7.1 Without robust information management procedures in place in relation to governance, there is a danger that the Council will fail to identify, understand, and monitor key strategic and operational risks. The consequence of this is that the Council could suffer enforcement action, legal challenge and resulting reputational damage or monetary penalties.

8.0 ENGAGEMENT/CONSULTATION

8.1 No specific consultation has been undertaken with regards to this report.

9.0 EQUALITY IMPLICATIONS

9.1 Wirral Council has a legal requirement to make sure its policies, and the way it carries out its work, do not discriminate against anyone. An Equality Impact Assessment is a tool to help council services identify steps they can take to ensure equality for anyone who might be affected by a particular policy, decision, or activity. No equality issues arising from this report.

10.0 ENVIRONMENT AND CLIMATE IMPLICATIONS

10.1 The content and/or recommendations contained within this report are expected to:

- Have no impact on emissions of Greenhouse Gases

APPENDICES

None

BACKGROUND PAPERS

Data Protection Policy
Freedom of Information Policy
Information Governance Policy
https://www.wirral.gov.uk/about-council/freedom-information-and-data-protection/data-protection-policy

Records Retention and Destruction Policy
https://www.wirral.gov.uk/result/?q=records+retention

SUBJECT HISTORY (last 3 years)

Council Meeting	Date
Audit & Risk Management Committee	
General Data Protection Regulation (GDPR) Implementation Update	12/03/2018
Council – Members and Acceptable Use Policy	18/03/2019

REPORT AUTHOR: Jane Corrin
ICT Governance and Compliance Officer (DPO)
Email: janecorrin@wirral.gov.uk