WIRRAL

AUDIT AND RISK MANAGEMENT COMMITTEE

Tuesday, 15 March 2022

REPORT TITLE:	**INFORMATION GOVERNANCE UPDATE**
REPORT OF:	**DIRECTOR OF RESOURCES (S151 OFFICER)**

REPORT SUMMARY

This report provides an update on the current work being done to sustain and deliver effective Information Management, relating to Information Governance across the Council. This work aims to reduce the risk of reputational damage and monetary penalties. The report also highlights areas of Information Governance work scheduled for the coming year.

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

RECOMMENDATION

The Audit and Risk Management Committee is 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. This report outlines current controls in place 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, as a public body is subject to The Data Protection Act UK 2018 which incorporates the requirements of the General Data Protection Regulation (GDPR). This legislation enhanced and strengthened the rights of individuals in relation to personal data and how it is collected, stored, used, shared, kept secure and destroyed. It also requires public bodies to be mindful of the rights and freedoms of individuals when processing their personal data.

3.2 The Council has a statutory Data Protection Officer (DPO), who acts independently of the Council in order 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 carried out prior to GDPR being enacted and this work was carried out in tandem with a review of Council websites to ensure compliance. As this review was a number of years back, the policies and procedures are now due for a further review and that has commenced January 2022 and is part of the IG work plan for the next 12 months.

3.4 Support for the DPO is given by Law and Governance department who specifically assist on complex Information Governance Issues. The Senior Information Risk Officer (SIRO) also supports the DPO by offering oversight and advice as required.

3.5 Many employees have now worked from home for between 18 months and 2 years and this shift has altered Information Governance risks and the mitigation required to minimise those risks. Although for many employees working from home is the new normal it is still important to be mindful of changing and emerging risks.

3.6 This report details key work undertaken in the past 12 months to help mitigate the changing risks in relation to Information Governance. It also gives details of work for the next 12 months which will help ensure the Council's compliance in a number of information management and data protection policy areas.

3.7 At ARMC on 30/11/2021 in relation to the SIRO report, several Councillor questions were raised in relation to Internal Reviews for Freedom of Information Requests and also Referrals to the Regulator, the Information Commissioner (ICO) for the period 2020/21, the additional detail given below answers those questions.

Internal Reviews - 2020/21
There were 21 Internal Reviews requested in this period.
17 of those were upheld and the requestors advised the next step in the process is to complain to the ICO if they remain dissatisfied.
4 were not upheld and these 4 internal reviews were undertaken because the requestor complained the request had been answered late. In such cases the review seeks to establish why the request was late and then advise the requestor. In addition, we review what help and assistance we can give to the service area. The number of internal reviews are relatively low in relation to the number of requests fulfilled but each one is reviewed independently of the original request.

ICO Referrals - 2020/21
During this period there were 6 cases reported to the ICO. The Council self-referred 1 incident in relation to a temporary health and social care worker and their processing of personal data. There were 5 public referrals:

3 in relation to subject access requests.
1 in relation to a school's admissions complaint.
1 in relation to a damaged paperwork being received.

In the period 2020/21, the ICO issued 1 decision notice in which they asked the Council to disclose some information it has previously deemed as commercially sensitive. This request had been subject to a robust Internal Review and the Council applied what they believed to be a comprehensive legal argument to not disclose the information.

Information Governance Risks

3.8 Two risks related to Information Management/Governance have featured on the Council's Corporate Risk Register for several years. These risks have the potential for wide ranging impact across the Council in terms of service delivery, financial and reputational damage. These risks are linked to risks on the Information Governance Board (IGB) Risk Register and are subject to regular review. The risks are currently recorded as:

- CRR20 - 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".
- CRR21 - 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".

Both of these risks were considered at the recent Strategic Leadership Team Risk Focus session on 2nd March 2022. The scores for CRR20 - Cyber Security are to be increased to reflect the potential for an increase in the threat of cyber-attacks as a potential impact of the war in Ukraine. There will also be a reassessment of CRR21 - Information Management to ensure alignment with changes to other Corporate

Risks. The changes to both risks will be fed through to the IGB Risk Register and monitored at the next Board meeting in April 2022.

3.9 The Information Governance Board (IGB), is chaired by the DPO and meets on a 6-weekly basis. It maintains its own risk register which is reviewed at each meeting. The risk register currently contains 13 risks which link directly to two risks within the Corporate Risk Register. The top scoring risks relate to:

The need to develop options for the long-term housing of the records management and archives service.

Poor management systems and the amount of unlisted and unmanaged information/ records in both paper and electronic form, and a lack of awareness and understanding of information management and information/cyber security responsibilities across Council, all of which have the potential to have large scale or wide-ranging impacts across the Council.

The work outlined in this report and activity planned in 2022 aims to mitigate and manage the risks. The IGB will continue to monitor these risks and escalate issues to the Corporate Governance Group and Senior Leadership Team as required.

IG Work in 2021/22

3.10 The work undertaken in the previous year/s in relation to Covid-19 led to a more connected partnership working between the Council and partner agencies such as NHS and Public Health England. This work helped the Council and partner agencies work more strategically together in the Covid related field. This work has continued into 2021/22 and there is still the requirements to draw up robust privacy notices which reflect and demonstrate new purposes why the Council needed to process data. These notices help the Council demonstrate transparency to the public on how and why they use people's personal data. These notices needed to be reviewed to ensure they were fit for purpose as Covid restrictions changed.

3.11 Covid also required a large number of Data Sharing agreements to be drawn up and agreed. These agreements were in relation to the Council working with partner agencies and charitable organisations. Review work was carried out on these agreements to ensure personal data was being held for an appropriate retention period.

3.12 The impact of COVID-19 has not completely gone away, although assumptions are that within 12 months there will be less impact on the teams related to Covid, this will be monitored and reviewed. The following current information and statistics help to demonstrate the variety and scale of the work currently being undertaken.

Statistical snapshot of Information Governance work

3.13 **Security Incidents**

3.13.1 The tables below provide a breakdown of the reported information security incidents and the incident severity assessment. The reported incidents for 2020/21 are provided for comparison.

	2020/21	2021/22*
April	10	12
May	14	8
June	13	12
July	8	14
August	14	5
September	13	21
October	12	18
November	16	19
December	7	18
January	10	13
February	18	10*
March	11	
	146	**150**

*As at 21 February 2022

The incident severity categorisation is assessed by the Information Security Incident Team. All incidents are discussed in a weekly meeting and severe cases are escalated to the relevant Service Manager for appropriate actions to be taken which could include changes to processes or refreshing staff training.

Incident Severity Assessment	2020 / 2021	2021 / 2022*
Severe	10	7
Moderate	37	32
Low	92	102
Informational	5	4
Undefined	2	0
Non-Incident	0	5
	146	**150**

*As at 21 February 2022

3.13.2 The increase in recorded incidents, over historical records, can in the main be attributed to the wider awareness of data protection arrangements following the introduction of GDPR in May 2018. This not only applies to staff who are required to and have undertaken training on Information Security and the requirement to report incidents in a timely manner but also the awareness and understanding of service users as to the requirements to ensure their data is held securely.
Information Security and the requirement to report incidents has had a higher profile since 2018 and service areas understand the need to report even on low level incidents.

The close monitoring of the security incidents have identified that there are weaknesses in areas which rely on accuracy of addresses they hold for customers, such as Benefits and Council Tax. As a result of having granular information on the security recording system some targeted work, such as GDPR training sessions has been undertaken and is further planned to ensure these incidents are minimised in the future. The planned work includes attending DMTs; plans for a suite of training on the new learning platform Flo and a planned session with the Councils Corporate Management Team and Strategic Leadership Team on where improvements can be made and to highlight any issues officers are facing that may be contributing to incidents occurring.

3.13.3 Determining the level of "Impact" of an incident is decided at the Security Incident Review Meetings with the Data Protection Officer, using advice and guidance from the ICO and the following statements are used as guidance:

Severe	The incident affected a large number of external persons The information involved was very sensitive The council incurred additional costs as a result of the incident The council experienced reputational damage as a result of the incident The incident was reported to the ICO or other regulatory body An external breach of one or more council systems was achieved
Moderate	The incident affected a large number of internal users The incident affected several external persons The information involved was extensive The incident included a formal complaint The incident involved significant time / effort to manage

Of the 7 incidents given an impact of 'Severe', 2 were self-reported to the ICO. The ICO decided not to take further action on one, and the other they decided that the 'offence was committed against Wirral Council' and the actions taken by Wirral Council were 'proportionate to any sanction that may be imposed by a court for an offence of this nature'. Of the other incidents given an impact of 'Severe', one undertook a disciplinary hearing with the member of staff who caused the incident, and others advised that team members would be reminded of the correct processes to be followed, to be vigilant and if required given training.

Of the 32 incidents given an impact of 'Moderate', 3 were self-reported to the ICO; all of which the ICO determined that no further action was necessary. A large number of 'Moderate' incidents occurred in Council Tax and Benefits and the Transactional Management Business Unit Manager met with the DPO on this issue and has now changed / updated processes and has recently provided new GDPR training for all members of staff in response to the increased number of incidents in this area.

The information recorded on all incidents is crucial to highlight patterns or weaknesses in processes, it is especially important to learn lessons from the security incidents and especially those graded as Severe or Moderate.

A review has already commenced in 2022 to ensure the processes relating to security incident reporting and monitoring is fit for purpose

3.14 **Referral to Information Commissioners Office (ICO)**

3.14.1 In 2021/22 the Council self-reported five information security incidents to the Information Commissioner's Office (ICO), all of which received the decision that no further action by the ICO was necessary. Some incidents reported are independent of the table above, as individuals may go directly to the ICO if they have a complaint. The ICO gave advice that although no action was necessary, they wished the Council to review the following: -

- Ensure People received adequate training
- Review related policies and procedures to ensure they were fit for purpose
- Review our Internal Complaints procedure to ensure it is fit for purpose

3.14.2 In relation to the period 20/21 referenced in the SIRO report presented to AMRC in November 2021, there were 6 cases referred to the ICO. The Council self-referred 1 incident in relation to a temporary health and social care worker and their processing of personal data. There were 5 public referrals:

- 3 in relation to subject access requests.
- 1 in relation to a school's admissions complaint.
- 1 in relation to a damaged paperwork being received.

In the period 2020/21, the ICO issued 1 decision notice in which they asked the Council to disclose some information it has previously deemed as commercially sensitive. This request had been subject to a robust Internal review and the Council applied what they believed to be a comprehensive legal argument to not disclose the information.

3.14.3 A plan to review all ICO referrals is due at the next meeting of the Information Governance Board and an action plan will be produced and monitored, and reported back to the committee via the Corporate Governance Group update.

3.15 **Requests for Information**

3.15.1 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. However, for financial year 21/22 and moving forward the figures are to a reporting schedule of requests received in the month, In terms of this there is a five week delay in reporting monthly figures.

	21/22 FOI's/EIR's received	**21/22 FOI's/EIR's responded to on time**	**% 21/22 FOI's/EIR's responded to on time**	**21/22 subject access requests received**	**21/22 subject access requests responded to on time**	**% 21/22 subject access requests responded to on time**
April	85	69	81%	19	14	74%
May	117	90	77%	31	21	68%

June	93	67	72%	11	10	91%
July	95	70	74%	19	11	58%
August	129	91	71%	24	17	71 %
September	123	93	76%	22	16	73%
October	134	103	77%	30	16	53%
November	135	105	78%	15	12	80%
December	89	69	78%	13	8	62%
January						
February						
March						
TOTALS	**1000**	**757**	**76%**	**184**	**125**	**68%**

3.15.2 Review and analysis of the subject matter of requests by the Information Management Team (IMT), allows for a review of what is included within the publications scheme, published on our web pages. The review of the scheme is continually undertaken to establish if there are any common FOI requests or emerging themes. If these are established then IMT can liaise with specific service areas to have this data published, to avoid the volume of similar FOI requests in the future. However, it is not possible to predict the volume of FOIs that are submitted, and some requests are so specific in nature that we wouldn't generally publish such data on the publications scheme.

Sometimes the information being requested is high profile but may be commercially sensitive or not available for publication until a certain time after consultation etc. For 2022/23 we are proactively assessing times when we carry out external communications to ensure that we can publish as much information in advance to minimise the number of requests being submitted as a result of these communications.

Requests for Internal reviews

3.15.3 If a requestor is dissatisfied with their response to an FOI request, the legislation allows then to request an Internal review of the response they received. In 2021/22 there were 21 requests for an Internal review. The information management team has begun to record more granular details in relation to the outcomes of internal reviews so this detail can be presented when requested to committee. The granular detail is given below:

- 11 were upheld and the requestors advised the next step in the process is to complain to the ICO if they remain dissatisfied.
- 5 resulted in further data being provided to the requestor.
- 4 were the result of the request being answered over the timescale.
- 1 currently remains open and is being processed.

Contrasting this with the period for 2020/21 there were also 21 Internal Reviews. 17 were upheld and the requestors advised the next step in the process is to complain to the ICO if they remain dissatisfied. 4 were not upheld and these 4 internal reviews were undertaken because the requestor complained the request has been answered late. In such cases the review seeks to establish why the request was late and then advise the requestor. In addition, we review what help and assistance we can give to the service area. The numbers of IRs are relatively low in relation to the number of requests fulfilled but each one is reviewed independently of the original request.

Actions by the ICO

3.15.4 The ICO has not issued any monetary fines against the Council for the period 2021 to current date, but they did advise the Council in relation to 1 Internal Review that they needed to revisit the request and answer in a timely fashion. This action was carried out and the Internal Review closed. The ICO also advises after any Internal Review is escalated to them that the organisation in question should:

- Ensure People who handle personal data are appropriately trained and have access to specialist advice of they require it.
- Ensure IG related policies and procedures are up to date and fit for purpose
- Ensure their Internal Complaints procedure has been reviewed and is fit for purpose.

Archives Service Statistics

3.15.5 The Archives search room was closed throughout the pandemic, reopening to the public 25 October 2021. Between this date and late February 2022, it has seen 157 visitors for whom 3592 documents were produced. Archive enquiries were received throughout the pandemic and 253 of these were answered remotely between April 2021 and late Feb 2022.

Records Management Statistics

3.15.6 For much of the last year, Records Management has continued to play a key role supporting Asset Consolidation and Staff Relocation (ACSR), clearing records from buildings whose staff now worked from home. This saw 850 boxes of material transferred into the records management facility, most in the period April to September 2021. Since then, the transfer of paper records to the facility has slowed significantly, reflecting the large-scale digitisation of Council services and operations.

The significant amount of material transferred during ACSR constitutes a large backlog of records awaiting processing by Records Management. This process is ongoing.

The demand from council officers to access records from the facility remains, with some 290 records on average being retrieved each month. Records are not permitted at home, retrieved records instead being digitised and delivered digitally where possible; where this is not feasible, officers come into Cheshire Lines to access records. Typically, between 20% and 30% of paper records requested are delivered digitised. This digitisation will increase and become the norm as more employees remain working from home.

Appraisals of records

3.15.7 During 2021 the clearing buildings of records has involved the time-consuming appraisal of many documents for archival value. This year some 227 boxes were appraised, significantly reduced from last year's number of more than 2,200 boxes.

Future plans

3.16 The legacy demands of the COVID-19 response have naturally led to some Information Governance tasks being delayed. However, 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:

- A Deputy Data Protection Officer has been recruited and commenced with the Council March 2022.
- Plans are underway to secure an additional full-time employee on the Information Management team; currently employed as part time.
- A wholesale review of Information Management policies and procedures commenced January 2022 to ensure they remain fit for purpose and reflect best practice.
- Ongoing use of communication channels for staff awareness messages to remind them of the responsibilities everyone has.
- During late 2021/22 a review of the Councils processing activities commenced, reviewing and mapping all our processing activities and recording them on a central register called a Record of Processing Activities – ROPA. The Council is required to have a ROPA and for it to be available for inspection by the Information Commissioner on request.

3.17 In relation to the ongoing mitigating and managing risks in relation to Cyber Security, the following activities are planned or already in progress:

- Collaboration with the Department for Levelling Up Housing and Communities Local Digital Cyber team to identify and implement improvements.
- Use of National Cyber Security Centre services, such as Early Warning, to detect and defend against malicious activity.
- Decommissioning and replacement of legacy infrastructure.
- Participation in Local Resilience Forum Cyber Resilience Working Group to share best practice and develop responses.

3.18 With regard to compliance with Data Security and Protection Toolkit (DSPT), this is an annual self-assessment for health and care organisations. The Council and any other organisations which have access to NHS patient data and systems must comply with the requirements of the toolkit. This compliance demonstrates and provides assurances that the Council are committed to and practicing good data security and that personal information is handled correctly. Failure to comply with the DSPT requirements could impact on your ability to access NHS patient data.

From 2022 onwards the self-assessment process and compliance requirements were in part moved to be owned by Health and Social Care, with advice and support to complete the toolkit available from key officers within ICT. The administration of DSPT toolkit remains within Information Management. The Council is currently compliant with DSPT.

4.0 FINANCIAL IMPLICATIONS

4.1 Although there are no immediate financial implications arising directly from this report. There could be financial implications if the Council's compliance is not adequate, which would lead to further risk of the Council's financial resilience.

5.0 LEGAL IMPLICATIONS

5.1 Public Bodies have a statutory duty to appoint a Data Protection Officer. This Officer plays a key role in monitoring internal compliance and is required to inform and advise on data protection obligations. They 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 is required to act independently and should be 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 Council's transparency when processing information. The DPO also has a pivotal 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 and policies 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

11.0 COMMUNITY WEALTH IMPLICATIONS

11.1 The content and/or recommendations contained within this report have no direct implications for community wealth. However, the delivery of an effective internal audit service will assist in ensuring that the Council, its finances, and service provision are effectively managed and governed aiding the advancement of economic, social and environmental

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

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 (SIRO Report)	30th November 2021
Audit & Risk Management Committee (Information Governance Update)	9th March 2021
General Data Protection Regulation (GDPR) Implementation Update	12/03/2018
Council – Members and Acceptable Use Policy	18/03/2019