AUDIT AND RISK MANAGEMENT COMMITTEE
TUESDAY 30 NOVEMBER 2021

REPORT TITLE:	**SENIOR INFORMATION RISK OWNERS (SIRO) ANNUAL REPORT**
REPORT OF:	**DIRECTOR OF LAW & GOVERNANCE**

REPORT SUMMARY

This report presents the annual Senior Information Risk Owners (SIRO) report. This type of report is seen nationally as good practice to inform Senior Leaders and Members of information governance challenges and to satisfy regulatory requirements.

It ensures continued compliance with the current information management legislation and regulations. These include The Data Protection Act 2018, The Freedom of Information Act 2000 and Environmental Information Regulations 2004.

The Senior Information Risk Owners Annual Report is attached at Appendix 1.

RECOMMENDATION/S

Members of the Audit and Risk Management Committee note the report.

SUPPORTING INFORMATION

1.0 REASON FOR RECOMMENDATION

1.1 To provide the Members with assurance that the Information Management Team is taking appropriate measures to comply with statutory requirements of Information Management Legislation.

1.2 To provide Members with assurance that the requirements of the Transparency Code are being met.

1.3 To provide further assurance to Members that security incidents are reported effectively and recorded with reference to the Information Commissioner as required.

2.0 OTHER OPTIONS CONSIDERED

2.1 The report has been submitted at the requested of the Committee who requested an update on Information Governance and associated risks within the Council, as such, no further options have been considered.

3.0 BACKGROUND INFORMATION

3.1 In 2020 The Information Governance Board greed to the production of a SIRO report, every 12 months. The report is designed to give assurance to Members that the Information Governance responsibilities the Council has are being met.

4.0 FINANCIAL IMPLICATIONS

4.1 There are none arising from this report

5.0 LEGAL IMPLICATIONS

5.1 The report discusses the work of the statutory role of the DPO and the SIRO and the expectations placed upon them.

6.0 RESOURCE IMPLICATIONS: STAFFING, ICT AND ASSETS

6.1 There are none arising from this report.

7.0 RELEVANT RISKS

7.1 Appropriate actions are not taken by officers and Members in response to the identification of risks to the achievement of the Council's objectives.

7.2 Potential failure of the Council to comply with the mandatory requirements of current relevant Information Management Legislation can result in monetary fines and reputational damage.

7.3 Potential failure of the Audit and Risk Management Committee to comply with best professional practice and thereby not function in an efficient and effective manner.

8.0 ENGAGEMENT/CONSULTATION

8.1 The content of the report has been reviewed and presented to the Information Governance Board. The report will be produced once every 12 months.

8.2 The content of the report has been reviewed and presented to The Corporate Governance Group.

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.

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 CO2/greenhouse gases.

11.0 COMMUNITY WEALTH IMPLICATIONS

11.1 There are none arising from this report.

REPORT AUTHOR: **Jane Corrin**
ICT Government and Compliance Manager – Data Protection Officer
0151 691 8645
Janecorrin@wirral.gov.uk

APPENDICES

Appendix 1 SIRO Report

BACKGROUND PAPERS

None

SUBJECT HISTORY (last 3 years)

Council Meeting	Date

Appendix 1

Contents

Executive Summary

This report presents the annual Senior Information Risk Owner (SIRO) report. This type of report is seen nationally as good practice to inform Senior Leaders and Elected Members of information governance challenges and to satisfy regulatory requirements.

The report provides an overview of the Information Governance agenda across the disciplines of Information Governance, Cyber Security, Transparency Code and Records Management. This is the first year the report has been produced and demonstrates legislative and regulatory requirements relating to the handling, quality, availability, and management of information, including compliance with the Data Protection Act (2018), General Data Protection Regulations (GDPR), and The Freedom of Information Act (2000).
This report for the year 2020/21, provides an update relating to the responsibilities of Wirral Councils Senior Information Risk Owner (SIRO). This role is occupied by The Director of Law and Governance who also fulfils the role of Monitoring Officer. The report details activity and performance related to information governance, providing assurances that information risks are being effectively managed; details current activity and explains where improvements are required.

Wirral Council is committed to effective information governance and has worked hard to ensure robust arrangements are in place to ensure the council complies with legislation and adopts best practice. Governance arrangements are monitored and reviewed to ensure systems, policies and procedures are fit for purpose and emulate best practice. The Council is equally committed to ensuring all Officers and Elected Members understand the importance of information governance. This commitment ensures that information governance is everyone's business and is embedded as part of the Council's culture.

The report references the review of Information Governance Policies which was undertaken in 2021 and the creation of a redesigned comprehensive Record Of Processing Activities (ROPA).

Cyber security risks remain a real threat and mitigating those risks continue to present a challenge to the Council. How the Council manages those risks is contained within this report, including a summary to list action already undertaken and further activities planned. These future plans will help maintain and strengthen defences and enhance corporate resilience.

Performance in relation to information requests processed under Freedom of Information (FOI), Environmental Information Regulations (EIR) and Data Protection legislation is summarised in this report. The report also provides an update on changes implemented in this service area to strengthen the resources available to meet the high demand for requests for information and advice/support in relation to the legislation.

The number of data breaches reported for the time period April 2020 to March 2021 are shown in comparison with the number of incidents reported in the previous year. Breaches are discussed at bi-weekly meetings with the Data Protection Officer to

ensure continuous monitoring takes place to identify learning or process changes that may be required to reduce the risk of further breaches occurring.

Looking forward to 2021/2022 a number of actions have been agreed to ensure the governance framework remains robust and the Council is able to demonstrate its commitment to compliance. These actions include:-

- Recruitment of a Deputy Data Protection Officer
- Additional resources deployed into the Information Management Team
- Additional resources deployed into Special Educational Needs Team to help facilitate Information Requests
- Review and overhaul of Transparency Code requirements
- Review of all Information Governance Policies
- Creation of a redesigned Record of Processing Activities (ROPA)
- Responsibility of NHS Data Security Protection Toolkit (DSPT) to be shared between Health and Social Care and Digital.

1. Introduction

The SIRO Report reflects on the Council's information governance work undertaken during 2020/2021 and provides assurances that personal data is processed in line with current legislation. This includes:

- an overview of key performance indicators relating to the Council's processing of information requests within the necessary legal frameworks
- an update on the plans the Council has in place to minimise risk or improve current or future performance
- providing assurance of ongoing improvement to manage information risks.
- information on organisational compliance with, and performance against, the legislative and regulatory requirements relating to the handling and processing of information in respect of:

  - Data Protection Act 2018 including the requirements of UK GDPR
  - Freedom of Information Act 2000
  - Environmental Information Regulations 2004
  - NHS Data Protection Toolkit DSPT
  - Any Security Incidents requiring notification to the regulator – Information Commissioners Office (ICO)

2. Key Roles and Responsibilities

SIRO
The Director of Law and Governance is the Council's SIRO and is responsible for:

- Leadership and overall ownership of the Council's Corporate Governance Action Plan, acting as corporate champion for information governance
- Providing a focus for the management of information governance at a senior level

- Providing advice and reports in respect of information incidents and risks, including the content of the Council's Annual Governance Statement relating toinformation risk
- Owning the management of information governance and risk assessment processes within the Council
- Understanding how the strategic priorities of the Council may be impacted by information governance risks, and how these risks need to be managed including the adequacy of resources and levels of independent scrutiny

DPO

The ICT Governance and Compliance Manager is the Data Protection Officer and is responsible for:

- Ensuring the Council's implementation of policies, standards and procedures for Information Governance ensures reduced risk of legal action from either individuals or regulators
- Creating and maintaining the Council's statutory records of data processing activities and information asset register to ensure the Council is not acting outside of its powers
- Acting as the prime contact with the ICO and individuals in the investigation of data protection complaints and breaches to reduce the risk of monetary penalty, legal enforcement, and reputational risk
- Identifying key control failings / weaknesses and provide support to senior managers to adopt new practices and procedures to improve operational performance and reduce risk.

The Data Protection Officer (DPO) has a dotted line of responsibility to the SIRO and both roles are based within the Resources Directorate. The DPO and SIRO meet on a regular basis to ensure any existing or potential issues relating to Information Governance are discussed and appropriate actions put in place.

In addition to these key Officers, there are a number of statutory and non-statutory Officers across service areas offering professional expertise in relation to information governance and information security. It is important that the Council embeds a culture that information governance is everyone's business, with all Officer and Elected Members taking personal responsibility to ensure information and data is held securely, processed appropriately and safely destroyed when not required.

Information Asset Owners and Administrators

The Council has many information assets which are defined as a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. An asset can be a single significant document or a set of related data, documents or files; it can be shared or be confined to a specific purpose or organisational unit.
Examples of information the Council is responsible for include - electronic customer/client records for example CRM files, case records in the social care system, audit records, paper records and reports, investigations, databases and data files, and others.

An Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core Information Governance (IG) objective that all Information Assets of the organisation are identified and that the business importance of those assets is established. There may be several IAOs within a council Directorate, whose roles within that Directorate may differ. IAOs will work closely with other IAOs of the organisation to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation. IAOs will support the organisation's SIRO in their overall information risk management function as defined in the council's Information Risk Policy.
The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAO will therefore document, understand and monitor:

- What information assets are held, and for what purposes
- How information is created, amended, or added to over time
- Who has access to the information and why
- Understand and address the risk to the asset, providing assurance to the SIRO

The Information Asset Administrator's (IAA) primary role is to support the IAO to fulfil their responsibilities. IAAs will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date.

3. Governance and Monitoring Arrangements

The SIRO is supported via two key groups: the Corporate Governance Group (CGG) and the Information Governance Board (IGB). The CGG, chaired by the Director of Resources, is a high-level strategic group that seeks to ensure proper arrangements are in place for the oversight of Information Governance matters within the Council. This includes receiving updates on key issues from the IGB.

The IGB, chaired by the DPO, monitors Information Governance performance and promotes Information Governance across the Council.

More specifically the responsibilities of the IGB are:

- Ensure that effective information governance / risk management and IT governance arrangements are in place across the Council.
- Ensure that the Council complies with statutory information governance provisions and that these are being applied across the Council.
- Embed a culture of information ownership and accountability throughout the Council.
- Ensure that the Council adopts industry best practice and aligns its work programme to the Council's strategic objectives.
- Share intelligence, identify opportunities for joint working and support management teams to identify baselines for improvement.

4. Risk Management and Assurance

The Council's Corporate Risk Register contains two risks in relation to Information Management and Cyber Security. Both of these risks are monitored via the IGB Risk Register which also contains risks 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 IGB Risk Register is reviewed at each meeting and used to identify priority areas to focus resources and carry out additional actions to help mitigate the risks.

Risks which are affected by activity outside the remit of the IGB, as well as areas of non-compliance are escalated to the Corporate Governance Group.

Part of the assurance of the Council's arrangements is carried out by the Internal Audit Team, which has a dedicated IT Programme Auditor. Recent audit reviews have included Cyber Security, Security Controls within Treasury Building all with a series of recommendations and timetable for completion.

5. COVID19

Ongoing Impact of COVID-19

It is hoped that Covid-19 will not dominate future SIRO reports, but it is appropriate to mention it in this specific report.

From early 2020 coronavirus (COVID-19) was spreading across the UK and had a massive impact on the delivery of Council Services in general and ICT services in particular: -
There was an increase in cyber-attacks and cyber fraud globally, nationally and regionally.

The revised flexible working environment and the need to social distance led to an increased reliance on the use of technology to maintain operations across the whole Council.

Wirral Council remains fully committed to ICT and cyber security and has implemented significant additional resources and overcome a number of operational challenges to ensure the Council responds effectively to COVID-19.
During 2020/21 and especially in context of COVID-19, an Information Security risk will remain on the corporate risk register to ensure we address the risks relating to accidental data loss, physical system failures and direct malicious cyber-attacks. There is an ongoing need for the Council to address all aspects of this risk through robust ICT and risk management processes as well as addressing the cultural and behavioral elements of this risk.

Covid-19 actions in relation to Data Protection has seen work undertaken by a range of colleagues/teams across the council and external/partner agencies, the non-exhaustive list below provides an insight into this activity:

- Control of Patient Information (COPI) Notices issued by Dept of Health and Social Care.
- Information Commissioner's Office (ICO): COVID19 Guidance.
- Data Sharing Agreement/Privacy Notice/Data Collection Forms required updating or producing across many service areas.
- Data Sharing Agreement/Privacy Notice for COVID-19 LocalContact Tracing System.
- Extensive Collaborative work with Cheshire and Merseyside Health and Local Authority colleagues.
- Extensive Collaborative work with numerous charities and initiatives to ensure goods and services were available to vulnerable groups.

It is of note to remember that Wirral Council's involvement with Covid19 was the first in the Country and we sought to support people evacuated from Wuhan. 31st January 2020 saw 83 Britons evacuated out of Wuhan and housed at Arrowe Park Hospital. Also of note are the lessons learned by colleagues involved in the council's response to this emergency, specifically in relation to data sharing obligations and documentation. Key procedures have proved adequate and supported the council to comply with its data sharing requirements throughout the COVID-19 response.

6. Corporate Governance Actions

The council is committed to a clear strategy and sustainable framework for Information Governance across the council. Performance reports are made available via Dashboards to the Senior Leadership Team to enable continuous monitoring of the actions required to manage information issues, risks and cultural behaviour to improve the Council's arrangements around data handling, processing and security.

In summary, the following key actions were delivered in 2020-21 which have strengthened the Council's management of information risks.

Staff in Wirral's Adult Care and Health are required to complete essential training called 'NCSC Staying Safe Online' on an annual basis. A performance high of 98% was achieved against the Council's target of 95%. The course was developed by the National Cyber Security Centre and completion of the course is also categorised as essential for all other staff throughout the Authority; this has been endorsed by the Council's Chief Executive.

The NHS requirement for an annual submission to be provided by the authority to show compliance with their Data Security & Protection Toolkit was extended to 30 June 2021 for 2020/21, however Wirral has provided it's submission on 23 March 2021.

The Council's Data Protection Officer chairs a bi-weekly meeting to consider all data breaches reported and advises on whether a self-referral of the incident to the Information Commissioner's Office(ICO) is appropriate.

The Data Protection Officer / ICT Governance and Compliance Manager, and the Information Governance and Security Officer have also undertaken the following additional and more in-depth training which is pertinent to their roles:

Data Protection Officer / ICT Governance and Compliance Manager
ICO DPO Conference in April 2020
North West Legal Consortium Data Sharing Seminar in November 2020
ICO UK/EU Transition Training session Brexit in December 2020

Information Governance and Security Officer – 5 day CISSP (Certified Information Systems Security Professional) course in September 2020.

7. Data Breach Management and Reporting

Any concerns relating to potential data breaches are promptly investigated and assessed against the ICO guidance. The key assessment includes a review of numbers of people affected, sensitivity, nature of breach and likely impact. Dependent on the assessment, the incident may need escalation to the SIRO, Caldicott Guardian, and maybe self-referred by the Council to the Information Commissioner's Office (ICO). The reporting, containment actions, investigation and learning phases of data breach incidents play a key role in the management of risk and improvement of internal controls.

All breaches and near misses are reported to the Data Protection Officer on a bi-weekly basis. Consideration is given to whether the incident should be referred to the Information Commissioner's Office (ICO). A total of eight cases were referred to the ICO in 2019-20. All these cases have since been closed by the ICO without any fines being applied. The ICO may make recommendations as a result of any investigations they undertake as to what actions they expect to be taken by the Authority.

During the period of 1st April 2020 to 31st March 2021, the Council recorded and investigated 146 potential data breaches. (In 2019 to 2020 there were 137 investigations undertaken). 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 as is shown in the table below. This not only applies to staff who 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.

Recording Year	Number of Incidents	GDPR?
1st April 2015 – 31st March 2016	40	No
1st April 2016 – 31st March 2017	60	No
1st April 2017 – 31st March 2018	73	No
1st April 2018 – 31st March 2019	127	Yes
1st April 2019 – 31st March 2020	137	Yes
1st April 2020 – 31st March 2021	146	Yes

The following Categories are used to record within the Security Incident Register, these categories and numbers of each potential breach are outlined below.

Category (from Register)	Number 2019/20	Number 2020/21
Undefined	1	1
Disclosure	104	102
Loss of Physical Asset	14	10
Unauthorised Access	4	4
Phishing	1	16
Denial of Service		2
Sensitive Information Lost	6	1
Other	7	10
Total	137	146

A further breakdown of incidents to give more detail and clarity are shown below.

Category of Potential Breach	**Number 2019/20**	**Number 2020/21**
Data posted or emailed to incorrect recipient	60	63
Failure to redact data	1	1
Loss / Theft of mobile device	15	10
Loss / Theft of paperwork	1	
Data left in insecure location	7	1
Verbal disclosure		
Near miss / Non event	2	5
Unauthorised system access	3	6
Failure to use 'Bcc' option when sending an email	6	4
Information uploaded to webpage	1	1
Disclosure of sensitive / personal data	15	5
Other failure		
Insecure disposal of paperwork		
Not applicable		
Request by Police	2	
Wrong Information Sent or Provided	16	18
3rd Party Breach	4	7
Incorrect use of Calendars	2	
Spam Email or Phone	2	16
Denial of Service / Website Down		2
Teams / Zoom / Social Media		7
Total	**137**	**146**

Learning from breaches:
As part of the investigation of an incident, learning actions will be captured to identify opportunities to reduce the chances of a similar breach occurring in the future.

This may see additional steps incorporated into a process before documents are issued, standard templates created to avoid the inclusion of incorrect information or post being issued via recorded delivery where appropriate.
Learning is shared across the organisation via either specific service area training or as corporate messages being issued to staff to remind them of good practice in avoiding breaches occurring.

8. ICT Security & Cyber Risks

The use of digital information and networks continues to grow and provides the foundation on which front line services are delivered. Cyber security continues to be a Tier 1 risk to national security. “Hostile attacks upon UK cyber space by other states and large scale cybercrime”. As such it remains of high importance and corporate priority.

The type of risks include theft of sensitive corporate or personal data, theft or damage to data, threat of hacking for criminal or fraud purposes and potential denial of service disruption to council ICT systems, intranet, mobile smart devices, public facing websites and misinformation.

Ongoing ICT Cyber Security Threats - Cyber-attack internationally, nationally and regionally remains a high risk overall and the actual consequences of a cyber-security attack on the Council, if realised,would be significant and have a considerable impact across all Council Services. Knowing how significant the impact of an attack like this would be, the Council has continued to strengthen information security controls to minimise the likelihood of an external cyber-attack.

Internal Audit are currently reviewing the remote access systems known to have been the target of cyber attacks in other Local Authorities during the sudden transition to pandemic-related home-working.

Wirral Council is working towards achieving Cyber Essentials Plus accreditation which provides a Good Practice framework against which risks, controls and progress can be tracked, and an independent assessment of the Council’s security. To reduce the risk still further the Authority has adopted the following approaches: -

The Council subscribes to and proactively participates in the iNetwork – North West Warning, Advice and Reporting Point (NW WARP). This group continually reviews cyber threat situational awareness and acts as a reporting and escalation mechanism for cyber incidents as well as providing mutual help, guidance and peer review. It is supported by the NCSC and facilitates access to the Head of PSN and to national cyber security expertise and support.

The Council’s presence on the external, public internet is registered and monitored bythe NCSC. Alerts are provided to Wirral Council to identify where weak configuration controls are identified which could be exploited. The Council is in the process of moving to the NCSC’s Protective DNS service which will stop people from accessing external web services which are known to be malicious.

As part of the commitment to cyber security good practice a robust patching regime is in place for Windows updates.

The Council employs an ad hoc scanning tool “NESSUS” and have a Security Group task to implement a more comprehensive scanning routine.

9. Freedom of Information & Environmental Information Regulations

During 2020-21 the Council received requests for information under the Freedom of Information Act and the Environmental Information Regulations. The number of requests is relatively constant and does not vary greatly year on year.

Year	Requests Received	Processed on time	Target 85%
2017/18	1337	1098	82%
2018/19	1573	1122	71%
2019/20	1487	1070	72%
2020/21	1256	1013	81%

In 2020/21 the Council responded to 1013 requests within the statutory time limit of 20 working days which represents a slight increase in performance compared with 2019-20. This is good progress as it should be noted that due to the impact of Covid-19 on services it was agreed not to pursue front line services for FOI responses during this period. This approach was echoed in advice issued by the regulator the ICO who said they would take a pragmatic approach and not penalise organisation's who struggled to meet time scales for requests.

The Information Management Team (IMT) records and ensures fulfilment of FOI and EIR requests. They proactively review request themes on a weekly basis to ascertain if any key or repeated themes are emerging. If so they are then able to alert service areas to that theme/high numbers of requests on a certain subject. This enables service areas to provide key information to IMT, which reduces the amount of time the team needs to repeatedly interact over the same subject matter. The service area may also choose to publish more information on the Council web site, which helps informs the public.

IMT proactively ensure that where possible information which is asked for on a regular basis is included in the Council Publication Scheme; thereby enabling the public to be signposted to publicly available information.
Publication scheme | www.wirral.gov.uk

This approach is echoed within the information which the Council publishes under the Transparency Code. This information includes information which is statutorily required to be published and also some additional data sets.
https://www.wirral.gov.uk/about-council/freedom-information-and-data-protection/publication-scheme/transparency-code

10. Data Protection Act (DPA) 2018

Under the Data Protection Act 2018, any living person, regardless of their age, can request information about themselves that is held by the Council. This application process is referred to as a Subject Access Request (SAR). In the past 2 years the council has handled the following requests.

The performance shown is against the target to process 85% within a calendar month.

	2019/20	2020/21
Requests Received	99	80
Actioned within 1 Month(Number)*	71	44
Within 1 Month (%)*	72%	55%

The Information Management Team (IMT) based within ICT Digital service receives and records all requests for data in relation to all service areas. In relation to SARs, Children's and Adults Social Care are responsible for collating and providing the responses directly. They have access to the data held in Liquid Logic and have the specialist knowledge and expertise required to identify what data should be/already has been shared. IMT provides advice and support in relation to any exemptions that may apply under the DPA 2018.

The low % statistics for 20/21 have been flagged up and recognised by the relevant service areas which are Special Educational Needs (SEN) and Adult Health and Social Care. Both service areas have obtained additional resources to assist with the current backlog. The large number of SARs has proved challenging in terms of maintaining the performance target during an already difficult year with Covid related work.

11. Internal Reviews

Customers who submit a FOI, EIR or SAR can request an internal review if they are not satisfied with the response provided. Internal reviews provide the Council with an opportunity to review the request handling process prior to any potential referral to the Information Commissioner's Office by the requester. During 2019-20 and 2020-21 the Council has processed the following Internal Reviews:

Internal Review Type:	2019/20	2020/21
FOI/EIR	60	21
Data Protection Act	2	1

The table reflects the change and improvement in working practices to try and reduce the amount of internal reviews which are carried out. Engagement with requestors is key in managing expectations and the Council operates a model of transparency.

12. Referrals to the Information Commissioner's Office (ICO)

If an applicant is not satisfied with the outcome of an Internal Review, they can refer their case to the Information Commissioner, who will assess the case and make an independent decision about the way the council has handled the request.
The role of the Information Commissioner is to uphold information rights in the public interest. The ICO is the regulator for Freedom of Information, Environmental Information Regulations and the Data Protection Act. Part of the Information

Commissioner role is to respond to complaints about the way local authorities have handled requests for information, make recommendations on best practice and take appropriate enforcement action. During the past year the Council notified the following referrals to the Information Commissioner:

Referral Type to ICO	**2020/21**
Freedom of Information	1
Environmental Information	2
Data Protection Act	3

Following a referral and a subsequent case investigation, the ICO can issue a Decision Notice requiring the Council to disclose information it may previously have refused to disclose. Details of all decisions received are monitored by the Data Protection Officer and reviewed by the Information Management Team in tracking response progress as well as lessons learned where the Council may be found at fault with the actions it has taken. In 2021 there was 1 Decision Notice issued from the ICO.

13. Referrals to the First Tier Tribunal (FTT)

If an applicant is dissatisfied with the Information Commissioner's decision, they have the right to refer the matter to the First Tier Tribunal (FTT). The council can also appeal fines issued for data breaches and enforcement notices to the FTT. The FTT is independent of the Information Commissioner and listens to representation from both parties before it reaches a decision. Any party wishing to appeal against an ICO Decision Notice has 28 days to do so.

During 2020-21 the Council did not receive or make any referrals to the First Tier Tribunal:

Referral type to FTT	**2020-21**	**Outcome**
Freedom of Information	0	Not applicable
Environmental Information	0	Not applicable
Data Protection Act	0	Not applicable

14. Information Governance Policies and Procedures Review and Creation of Record of Processing Activities

Commencing in May 2021 a comprehensive review of all Information Governance policies and procedure documents was undertaken to ensure that Council staff have up to date and adequate guidance to comply with statutory requirements. Authors and owners of the policy documents were contacted and asked to review, to ensure the policies and procedures were still required and if so that the content was up to date and reflected current legislation and best practice.

Approximately 100 documents have been identified, and the review is underway, it includes content on the updated Intranet. This key piece of work means the web

content of Information Governance polices will be refreshed and updated by the end of 2021 with relevant review dates included for the next review and refresh.

Alongside this piece of work, the Council also is required to have an up to date comprehensive ROPA to give assurance to the Information Commissioner's Office that they were complying with the requirements of Data Protection Legislation. The ROPA is a living document which details a granular level of data processing information for an organisation.

The ROPA project involves extending the existing Information Assets Register the Council has been using, adding additional information re; information assets and attaching process and controls information to those assets. This enables the Council to have adequate insight into the main areas of risk in the area of data / information assets to help mitigate the risk of data incidents and / or breaches etc occurring in the future. The project also includes Non Personal Data to encompass all Council data and not only personal data.

15. Conclusions

In summary, good progress has been made during 2020/21 with key actions taken to strengthen the Council's approach to effectively manage information risks and ensure a robust approach to information governance. In particular, as the potential for cyber risk increases, it is essential the Council takes action to understand and mitigate risk in this area.

Information Governance is highlighted within the Corporate Risk register and the regular meetings of IGB and Corporate Governance Group, coupled with regular meetings between the SIRO and DPO all demonstrate the commitment the Council has to maintaining and improving effective Information governance.

The Corporate IMT now meets regularly with Health and Social Care, Health Trusts and CYP representatives to share knowledge and offer support in relation to information management requests. This ensures a coordinated agreed approach is taken when responding to complex requests for information.

A full review of Information Governance policies is underway and a new ROPA is being produced.

Further Information - For further information and guidance please contact:

- SIRO - Philip McCourt Director of Law and Assurance
  Philipmcourt@wirral.gov.uk

- DPO - Jane Corrin ICT Governance and Compliance Manager DPO
  Janecorrin@wirral.gov.uk

- IT Security Officer - Judith Barnes
  Judithbarnes@wirral.gov.uk

- Information Commissioners Office website https://ico.org.uk/
  Information Commissioners Office Contacts https://ico.org.uk/global/contact-us/