WOKINGHAM
BOROUGH COUNCIL

Senior Information Risk Owner (SIRO)

Annual Report
Review for the Financial Year 2022/23

Version 4.1; 4th July 2023

Contents

Executive Summary

This report presents the annual Senior Information Risk Owner (SIRO) report. This role is occupied by the Assistant Director Governance who also fulfils the role of Monitoring Officer. 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 SIRO has responsibility for understanding how the strategic business goals of the organisation may be impacted by any information risks and for taking steps to mitigate those risks.

The report provides an overview of the Information Governance agenda across the disciplines of Information Governance and Cyber Security and provides assurances that information risks are being effectively managed. This is the first year the information contained has been produced in this format (as a single report) and demonstrates legislative and regulatory requirements relating to the handling, quality, availability, and management of information, including compliance with legislation such as the Data Protection Act (2018), General Data Protection Regulations (GDPR), Freedom of Information Act (2000), and Environmental Information Regulations (EIR).

The report outlines activity and performance related to information governance for the period of 1st April 2022 to 31st March 2023, and identifies where improvements can be made, and any actions being implemented in the upcoming financial year.

1. Introduction

1.1 Wokingham Borough Council is committed to effective information governance ensuring that robust arrangements are in place for the Council's compliance with legislation and adoption of best practice. We view this as a continuous improvement cycle, where 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 seeks to promote the ethos that information governance is everyone's business and is embedded as part of the Council's culture.

1.2 IT security and cyber risks remain a real threat for organisations (locally, nationally, and globally), the cyber threat has increased in line with the ongoing war in Ukraine. The UK Government has warned that critical national infrastructure which we are part of is of particular interest to Russian state cyber activists. Mitigating cyber risks by working to enhance our resiliency remains a priority, we have engaged with a Cyber Security partner the Cyber Security Associates to actively monitor and advise. How the Council manages Cyber risk is outlined within this report, including a summary of action already undertaken and further activities planned. These future plans will help maintain and strengthen defences and enhance corporate resilience.

1.3 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 being implemented to strengthen the resources available to meet the high demand for requests for information and advice/support in relation to the legislation. This is work that will continue to be carried forward in 2023/24 as the Council continues to identify improvements that can be made.

1.4 The number of data breaches and concerns reported are shown in comparison with the number of incidents reported in the previous Financial Year. The Council have reviewed its processes, making changes when GDPR was introduced to ensure that we would be able to meet the requirements that the legislation set. We carried out a communications campaign and training regime which strengthened staff awareness and understanding of Data Protection and how to react should a data breach occur. The Council requires staff to carry out refresher training on Data Protection periodically, with a view to ensuring 100% completion in an appropriate timeframe.

1.5 Looking ahead to 2023/2024; a number of recommendations have been agreed to ensure the governance framework remains robust, and the Council is able to demonstrate its commitment to compliance. These actions include:

- Additional resources deployed into Children's Services to help facilitate Subject Access Requests and reduce the backlog
- Refreshing Information Governance Policies and adding new ones where any gaps are identified
- Reviewing the Council's Retention Schedule
- Reviewing and overhaul of Transparency Code requirements and data published on the Council's website in conjunction with the website upgrade
- Review of the Council's fees and charges relating to Freedom of Information, Environmental Information Regulations and Subject Access
- Any serious issues or concerns identified by the Internal Audit that will take place during 2023/24.

2. Key Roles and Responsibilities

2.1 It is important that the Council embeds a culture of recognising that information governance is everyone's business, with Officers and Elected Members taking personal responsibility to ensure information and data is held securely, processed appropriately, and safely destroyed when not required. Whilst all staff are responsible for information risk management and handling of personal data within their own service areas and teams, there are certain individuals who have specific responsibilities in respect of information risk management, which can be summarised as follows.

a. **Senior Information Risk Owner (SIRO)** is the senior officer with overall responsibility for information risk and has responsibility for promoting Information Governance policy within the Council. Acting as corporate champion for Information Governance, providing reports and advice in respect of information risk, and understanding how the strategic priorities of the Council may be impacted by said risk(s). This role is held by the Assistant Director of Governance.

b. **Data Protection Officer (DPO)** is charged with leading and direction the Information Governance activities across the Council, and reporting, as required to, by the SIRO. Acts as the primary contact with the Information Commissioner's Office (ICO) and individuals in matters related to data protection, ensures the Council's implementation of policies, standards and procedures for Information Governance, and identifies areas for improvement providing support to senior managers to adopt new practices and procedures to improve operational performance and reduce risk. This role is held by Information Governance Officer in Legal Services.

The DPO and SIRO roles are based within Governance Services in the Resources & Assets 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.

c. **Caldicott Guardian** is the senior officer within a health or social care organisation who ensures that the personal information of service users is managed in a legally, confidentially, and in an ethically and appropriate manner. A Caldicott Guardian provides leadership and informed guidance on complex matters involving confidentiality and information sharing of health and/or social care data. This role is held by the Director of Adult Social Care and Health.

d. **Corporate Leadership Team (CLT)** is chaired by the Chief Executive and 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. CLT will receive quarterly reports from the SIRO, including receiving updates on key issues from the DIGB, and provide their support when needed.

e. **Data Information Governance Board (DIGB)** is responsible for the oversight of information risk within the Council, ensuring that effective information governance, risk management, and IT governance arrangements are in place and disseminated to directorates. Embedding a culture of information ownership and accountability throughout the Council. The Board is chaired by the SIRO and meets monthly. Additional meetings are scheduled as required. Representatives from each directorate attend who are senior managers (either at Assistant Director level or their nominated representative if they are unable to attend), to allow decisions to be made in their Information Asset Owner roles. Other key roles in the organisation such as Head of IT, the DPO, and the Governance & Risk Manager attend to; feedback on, keep apprised of, and take any messages or actions to their respective service areas and teams.

f. **Information Services** is the Council's central team who process all information requests received and co-ordinate with other service areas; FOI, EIR, Subject Access, Police Enquiries (or other organisations requests), Data Breaches and Concerns related to Data Protection. The service provides advice, guidance and assistance to Officers in the Council on matters surrounding these

Information Governance topics, and manages data breaches ensuring any incidents are logged, investigated, and raising recommendations to the Information Asset Owners (and SIRO as required). This team sits within Legal Services.. Nominated solicitors from Legal Services carry out the Internal Reviews related to information requests as required.

g. **Information Asset Owners (IAOs)** are accountable for the information being created, received or obtained within their directorate, what the purpose of holding this information is for, and any associated information risks there could be and business continuity to mitigate/continue to operate in periods where assets are unavailable. They are responsible for ensuring that the Council's policies are implemented in their service areas, for ensuring that their staff are aware of the information governance policies that affect them and their staff complete training as required. To foster a culture of personal responsibility and commitment to information governance matters in their department. Wokingham Borough Council's IAOs are the Assistant Directors.

h. All staff, including temporary and agency workers, have a personal responsibility to handle information in accordance with Information Governance policy and Legislation, complete data protection and induction training and continue to complete refresher training periodically, and report any data security incidents, breaches and malpractices they encounter.

3. Risk Management and Assurance

3.1 The Council's Corporate Risk Register contains two risks relevant to this report; Information Management, and Cyber Security. Both risks are monitored and reviewed by DIGB and the Corporate Leadership Team.

3.2 The Information Management risk covers the Council's Publication Scheme and Access to information, our Policies and Procedures, Training, Data Breaches and Concerns, Networking with the other Berkshire Local Authorities, Records Management and Retention, Privacy Impact Assessments, and Data Sharing Agreements.

3.3 The Cyber Security risk covers the Council's access to physical equipment and electronic information including back up and business continuity, updates and upgrades to the Council's network and software, penetration testing of the Council's electronic security, awareness campaigns and simulated phishing campaigns, ensuring compliance with PSN certification, and membership and working with the relevant advisory groups or forums for the South East.

3.4 Part of the assurance of the Council's arrangements is carried out by the Internal Audit Team. Recent internal audit reviews have been carried out with IT to cover the Cyber Security Risk Register and an audit will be taking place in 2023/24 period to cover the Information Management risk. Any recommendations and actions arising will be time tabled and implemented as necessary depending on risk severity.

4. Data Breach Management and Reporting

4.1 The number of incidents reported provides evidence as to the awareness of the requirement to ensure data is held securely, processed in line with legislative requirements, and to report incidents in a timely manner when a potential breach occurs. Any concerns relating to potential data breaches are promptly investigated and assessed against Information Commissioner's Office (ICO) guidance. This is carried out by the Information Services team, where the Data Protection Officer role sits, and are assessed based on (but not limited to) sensitivity of information, type of recipient(s) (e.g. whether it's a professional organisation or member of the public receiving the data), number of people affected, nature of the breach and the likely impact.

4.2 The Council assesses breaches as *Low, Low-medium, Medium, Medium-high, and High*. We may also categorise concerns as *'None'* when the conclusion of investigation the allegations have not been substantiated, or if a third party has had a breach which does not affect Wokingham Borough Council residents' data but we have been informed as part of the third party obligations.

4.3 The Information Commissioner's Office (ICO) states that not all Data Breaches need to be reported to their organisation and their approach is that organisations take responsibility and accountability for minor breaches. The Council do not report breaches up to the Medium category to the ICO (with some exceptions dependent on case details) but carry out necessary actions and record them on their breach register (advised by the ICO to keep records). High breaches would require being reported to the ICO, which needs to be done within 72 hours, while Medium-High breaches we would contact the ICO helpline to discuss the case further to seek their view on the matter. The Officers in Information Services will also use the ICOs Breach Self-Assessment toolkit as reassurance to decisions made when necessary.

4.4 Following investigation and assessment of a data breach, the Information Asset Owner (IAO) is informed by Information Services *if* any process change, training or other learning actions are required when of a significant nature. The Line Manager or Service Manager are informed when the breach is low risk, or minor alterations are required, with their consideration whether to inform the IAO immediately. The SIRO and DPO discuss any significant breaches during their regular meetings, and this is included as a regular agenda item for DIGB detailing the previous month's breaches. From the start of 2023/24 an annual summary will also be provided to aid in spotting trends and patterns to plan ahead through the new financial year.

4.5 The Council recorded and investigated 106 instances of data breaches, alleged breaches, or concerns, during 2022/23.. This figure remained consistent with the previous year, and should be noted that it does not include Cyber Attacks against the Council that our IT Service experience and prevent (Like Denial of Service (DOS)). The risk of the breaches for the year have been categorised as follows;

High	Medium-High	Medium	Low-Medium	Low
0	0	7	17	80

4.6 During 2022/23, the Council submitted one report to the ICO. This related to a breach that was subsequently categorised as 'low-medium' risk.

Learning from breaches:

4.7 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.

4.8 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.

4.9 In 2023/24 and 2024/25, the Council plans to review and refresh how Data Breaches are catalogued when recorded to be able to monitor and filter these cases.

4.10 With the introduction of GDPR the Council implemented improvements and strengthened its data breach reporting, investigations, learning and monitoring. As a result we have seen an increase in the number of breaches that are being reported to the Information Services team, however at the same time the severity of the risk has been reduced, and the number of staff carrying out mitigating actions *before* reporting to Information Services has increased. These prompt actions taken by staff when discovering or being alerted to a data breach greatly reduce the risk to the Data Subjects of these breaches.

4.11 The Council will continue to promote good information governance practices through 2023/24, and messages to staff to ensure that they are aware of actions to take following a breach or suspected breach. This will also include the IT Services work in terms of Cyber Security and simulated Phishing Campaign(s).

5. ICT Security & Cyber Risks

5.1 The dependency on digital information and networks continues to grow and provides the foundation on which front line services are delivered. With a result of the Pandemic, the Council had to shift to remote working sooner than it had anticipated/planned, however the roll out and operation of this was a success. Officers have continued to work from home for the majority and the Council have moved to a hybrid model following the lockdowns and restrictions of Covid-19 pandemic where all officers (exception of some rolls) so there will need to be a more focused shift on the Council's estate. To ensure that Officers are able to access all information that they require to carry out their role, and as far as reasonably possible ensure the upkeep of the Council's network.

5.2 Cyber security continues to be a high risk nationally and in recent years we have seen councils increasingly be the targets and victims of these attacks. The Hackney Council cyber attack in October 2020 demonstrated that the consequences of a significant attack being successful could significantly impact an organisation's ability to operate. The cost of recovery (estimated at £12 million+) would have a significant impact on any councils budget, together with the impact on service delivery. As such, it remains of managing and mitigating the risk of cyber security remain a key corporate priority. Other recent cyber incidents impacting local government include Gloucester City Council and Capita whose Cyber incident resulted in several councils being able to deliver their Revenue and Benefits service for an extended period of time.

5.3 The type of risks includes theft of sensitive corporate or personal data, theft or damage to data, threat of being held to ransom for financial gain, 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. The Council is no different to other organisation and experience cyber-attack attempts on an almost daily basis. There are periods in the year or events that are taking place where it is known that the Council will experience an increase in attempts. Historically, we have seen increased cyber activity around election time.

5.4 The Council is working towards achieving Cyber Essentials Plus accreditation which provides an accreditation and good practice framework against which risks, controls and progress can be tracked, and an independent assessment of the Council's security. The Council has continued to meet its Public Services Network (PSN) accreditation for the 2023/24 financial year. As part of the commitment to cyber security good practice a robust patching regime is in place for Windows updates and IT continuously reviews and updates its Cyber response plan.

5.5 Cyber risk is included on the Corporate Risk Register and the Council's Internal Audit team has just completed its report and suggested actions. IT will be implementing this over the 2023/24 year while prioritising aspects that are considered high risk. Other items that IT have had involvement are detailed later in the report.

5.6 The Council received a £100k Cyber grant from DHLUC to fund approved projects to increase the Council's cyber resiliency.

5.7 The Council has engaged the Cyber Security Associates as its cyber-partner to provide a 24/7 security operations centre (SOC) to monitor for malicious cyber activity across the IT estate. As a partner, they have developed a cyber-incident plan for the Council and will be working with service areas to ensure this is integrated into their business continuity ahead of formally testing with an emergency planning event focussed on cyber.

6. Access to and requests for Information

6.1 The Council is committed to operating in an open, ethical, and transparent manner. Enabling residents, clients, and customers to scrutinise the way that the Council operates, ensures that we continue to utilise resource as effectively as possible, deliver the best possible services to residents and use public funds in the most appropriate manner. Individuals have a number of access routes to request data from the Council and escalate concerns to the regulatory body.

Freedom of Information (FOI) & Environmental Information Regulations (EIR)

6.2 Information Services records, monitors, and ensures fulfilment of FOI and EIR requests; all responses are quality assured by the team before being issued.. The team has worked with the SIRO to implement changes in 2022/23 to help the Council towards reaching its 90% on time response target which is set by the Information Commissioners Office.

6.3 As there can be overlap between these two pieces of legislation when a request is submitted, due to the questions posed or the information held, the Council reports on these as a combined statistic rather than attempt to separate them out. These avenues for requesting information share similar frameworks, and have the same timeframes for responding to a request which allow us to group these two pieces of legislation statistics together.

6.4 FOI and EIR activity remained relatively high throughout the year, although there were periods around the holidays (School breaks, Christmas, Easter, etc.) when the Council did see a drop in requests submitted. While we did see requests reduce during the pandemic, we have started to see that the submissions gradually increase and appear to be returning towards the pre-pandemic submission figures.

6.5 Whilst requests are applicant and motive blind, from the data available it is notable that residents comprise a relatively small proportion of total requests, the bulk of residents coming from the media, businesses, and students. We also receive requests from other organisations for bench marking purposes, Elected Members, and Central Government. The figures for the previous two financial years are as follows.

Year	Requests Received	Requests answered on time	Percentage (ICO target 90%)	Resources Cost*	Staff Hours^
2021/22	1140	967	84.8%	£38,074.98	1,523
2022/23	1052	940	89.4%	£32,445.80	1,298

The above figures may differ from the website, as we have removed duplicates, blank/spam bot web submissions, withdrawn requests, or non-related FOI/EIR contacts from the figures. Figures based on date due of request and not date received.

*Cost is only as accurate as staff record on the system. Only takes into consideration time which is applicable to be recorded under the FOI/EIR legislation, therefore doesn't reflect true costs involved.

^Hours is figure derived from 'cost divided by 25', as ICO sets £25 per hour, rounded to nearest full hour. We recognise this is not a true cost or time taken due to what is allowed to be recorded set by legislation.

6.6 Whilst the Council marginally fell short of the 90% target set by the ICO in 2022/23, there have been significant improvements in performance over the course of the year. We are confident that the measures put in place over the latter half of 2022/23 will continue through 2023/24 and that the Council will achieve the 90% target.

6.7 Wokingham Borough Council publishes its response to requests that we receive under FOI and EIR, along with other useful information.

- https://www.wokingham.gov.uk/council-and-meetings/information-and-data-protection/publication-scheme/
- https://www.wokingham.gov.uk/council-and-meetings/open-data/datasets-and-open-data/
- https://www.wokingham.gov.uk/council-and-meetings/information-and-data-protection/see-answers-to-previous-information-requests/

6.8 Looking ahead, Information Services are reviewing FoI requests received in previous years to supply to services a list of common and frequently requested information to further increase information already published which is commonly requested. This will be used to aid information demand and to proactively publish information that should be openly available. The Council's website is being updated in summer 2023 so this is an opportunity for the Council to increase the data being published with the refreshed website design.

Data Protection Act (DPA) 2018

6.9 Under the Data Protection Act and General Data Protection Regulations (GDPR) 2018, any living person, regardless of their age, can request information about themselves, known as a Subject Access Request (SAR), held by the Council.

6.10 The following figures are based on the elapsed time between submission and response noting that some requests are more complex and can be extended to 60 or 90 days. The within time limit includes those complex requests which have been extended to 90 days, and not just those requests answered within 30-day period.

	2021/22			**2022/23**		
	Received	**Responded in time**	**Percentage in time**	**Received**	**Responded in time**	**Percentage in time**
ASC	11	7	64%	16	9	56%
CS	76	21	28%	90	44*	49%
IS	32	24	75%	24	20	83%
Total	**119**	**52**	**44%**	**130**	**73**	**56%**

Adult Social Care and Health (ASC), Children Services (CS) and Information Services (IS). IS handle any non Children and Adult Services related requests, e.g. Housing, Council Tax, Human Resources.

*At the time of writing the report there are 17 requests which are still active and their due dates have not expired due to being extended to 90 days and being received in Q4 of 2022/23.

6.11 While it is clear that there is more work to be done within the Subject Access process, there have been reasonable achievements and improvements that have been made during the 2022/23 period as seen with the figures above, especially with cases relating to children.

6.12 Our priority for 2023/24 is to continue working on the backlog of requests that have built up within Children Services, with the aim to by the end of the 2023/24 period to have caught up with requests. We are balancing new requests against those which have been with the Council for a period of time already. Resource will be monitored, along with considerations about how the best way to process requests, meet demand, and complete requests within the rules of the legislation.

Schedule 2 Enquiries

6.13 There are exemptions within the Data Protection Act 2018 that allow organisations to submit 'Schedule 2' requests to the Council. These are requests for personal data usually submitted by the police, utility companies, or other Councils, and generally fall under either the 'prevention and detection of crime' (for police) or 'collection of a tax or duty' (everyone else).

6.14 The Council received 80 requests under Schedule 2 exemptions during 2022/23. This is an 18% increase form 2021/22 when the Council received 68 enquiries. Of the enquiries received. 91% were answered within a few days of being received. The Council's aim for 2023/24 is to reduce the number of requests which experienced significant delay, clarify the performance standard, andbuild more resilience in the process.

Internal Reviews

6.15 Applicants who submit an FOI, EIR, or Subject Access can request an internal review if they are dissatisfied with the response provided. This could be as a result of an incomplete answer, information being withheld under an exemption/exception, or undue delays in response. If the applicant remains dissatisfied with the Internal Review response, they are able to escalate their complaint to the Information Commissioner.

6.16 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 applicant and, if appropriate, correct the response that they received. During 2022/23 the Council has processed the following Internal Reviews;

- FOI/EIR: 7
- Data Protection Act: 3

6.17 The Council administers one thousand access to information requests each year and only approx. 1% required escalation to Internal Review. While we acknowledge that we will never reach zero internal reviews in any given year, as applicants have a right to request one, the figure demonstrates that applicants in the vast majority are satisfied with the responses provided. The Council's Information Services team in prior years implemented improvements to the process and quality assurance mechanisms being strengthened to reduce the amount of internal reviews being carried out by the Councils Legal Service. The aim for 2023/24 is to continue this working practice and keep review figures around the 1% figure.

Referrals to the Information Commissioner's Office (ICO) about information requests

6.18 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. They are also able to refer to the ICO should they believe that the Council are not handling their information governance duties appropriately. The role of the Information Commissioner is to uphold information rights in the public interest. 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.

6.19 The Council has not self- referred to the ICO (in relation to access to information) on any occasion during the 2022/23 period. To the Council's knowledge, none of the above Internal Reviews were escalated to the ICO: No decision notices against Wokingham Borough Council have been issued for 2022/23.

6.20 The Council, did however, also receive four contacts separately from the ICO in relation to Subject Access requests in which the applicant directly approached them to request the ICO's involvement. All four cases were in relation to the applicant being advised there would be a delayed response to their Subject Access and the ICO required the Council to complete these requests within 14 days from date of ICO contact. The Council complied with issuing a response to the applicant within the ICO's timeframe in all four instances. As mentioned in prior section the Council has taken measures to reduce and clear the backlog through 2023/24 period.

Referrals to the First Tier Tribunal (FTT)

6.21 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 considers representations from both parties before it reaches a decision. Any party wishing to appeal against an ICO Decision Notice has 28 days to do so.

6.22 During the 2022/23 Financial Year the Council did not receive or make any referrals to the First Tier Tribunal.

7. Information Governance Policies and Procedures

Internal Audit

7.1 The Information Governance service area is due for its internal audit during the 2023/24 period. This will review items such as policies and procedures, training, data breaches, access to information routes, publication scheme, retention and disposal regimes and any concerns from the previous audit. Anything that is identified as being high priority out of this audit will be actioned during 2023/24.

ICO Self-Assessment toolkits

7.2 To indicate where the Council stood in terms of Information Governance and IT Security in 2021/22 an ICO Data Protection Self-Assessment was undertaken. This informed the priorities for the year ahead and compared the Council's practices against ICO best practice. The Council will complete another Self-Assessment(s) at the end of the 2023/24 period and compare their progress and achievements against the prior assessment(s).

Data Information Governance Board (DIGB)

7.3 The Data Information Governance Board (DIGB) comprises senior officers from across the Council. The Board is responsible for leading and promoting the Council's information governance arrangements and reports regularly to the Corporate Leadership Team.

Policy and procedures

7.4 All staff are required to review and sign the Council's *'Information Security and Acceptable Use of ICT'* policy. This is supplemented by regular training in this area.. During 2023/24 the policy will be reviewed to ensure it continues to reflect best practice.

Internal training and communications

7.5 The Council refreshed its Data Protection eLearning content in 2022/23. Staff are required to complete full refresher training on Data Protection every two years. This year, rather than have every officer go through the training regardless of join date to the organisation all at once, Information Services worked with Human Resources to alter the training so that it would auto enrol individuals to take the training one month before their training certificate expired. This will allow for better monitoring and escalation of non-compliance.

7.6 The Council's Intranet on Data Protection will be refreshed and improved in 2023/24 with all information accessible in one location as a hub to make it simpler and quicker for staff to access the information, templates and guidance that they need.

Information Asset Register (IAR) and Register of Processing Activity (RoPA)

7.7 In 2018, in preparation for the introduction of GDPR, the Council reviewed information assets in depth and created its' RoPA.

7.8 A priority for 2023/24 is to review and refresh these registers. Work has begun in April 2023 to update the Excel based IARs with consideration to migrate these registers to a system in the future which will allow for better monitoring and updating.

7.9 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. This initial work and consideration is likely to continue into the 2024/25 financial year.

Information Sharing Agreements (ISA), Privacy Impact Assessments (PIA) and Software

7.10 Another priority for 2023/24 is to identify and catalogue and review all agreements.

Data migration and Document Management System

7.11 The Council is upgrading its Document Management system from Information@Work to NEC DM System, with a view during 2023/24 to also update the Document Management system used in Social Care to migrate to NEC DM. This will reduce the number of Document Management systems in use and also offer a consistent approach which should make it easier for officers to use and manage information. Retention will be added into the system which will allow for less reliance on officers manually removing data when its retention has been reached.

External Certificate

7.12 The Council has continued to maintain the required assurance certifications, such as Public Service Network (PSN) and NHS Toolkit. All these processes for external certification involve submitting evidence to the supervising Government body to show we comply with their requirements. Work has also commenced on Cyber Essentials, a government certification overseen by the National Cyber Security Centre and regarded as a key indicator of assurance. The Council will continue to maintain these external certifications, and we plan to monitor any news or updates as we understand that PSN may be replaced in future.

8. Corporate Governance Actions

8.1 The Council is committed to a clear strategy and sustainable framework for Information Governance. A number of actions have been identified throughout this report to be carried out during 2023/24 to further strengthen Information Governance. Next year's SIRO report will review the Council's achievements of these actions.

8.2 Throughout 2023/24 there will be continuous monitoring and updates to senior leadership about Information Governance, and the Council will adapt as needed to mitigate risk. This will be taken into consideration when the 2023/24 report is produced.

9. Conclusion

9.1 In summary, good progress has been made during 2022/23 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.

9.2 Information governance is highlighted within the Corporate Risk register and the regular meetings of DiGB and Corporate Leadership Team, coupled with regular meetings between the SIRO and DPO all demonstrate the commitment the Council has to maintaining and improving effective information governance.

Further Information - For further information and guidance please contact:-

- SIRO – Andrew Moulton, Assistant Director Governance
  Andrew.moulton@wokingham.gov.uk

- DPO – Stuart Bignell, Information Governance Officer
  Stuart.bignell@wokingham.gov.uk

- Head of IT – Glynn Davies
  Glynn.davies@wokingham.gov.uk