Senior Information Risk Owner (SIRO)

Annual Report 2022 - 2023

Report Summary

Producing an annual Senior Information Risk Owner (SIRO) Report is seen nationally as good practice, its aim is to inform Senior Management and Elected Members of information governance challenges and raise awareness of the Council's regulatory obligations.

Furthermore, the report aims to provide assurance of compliance with the council's statutory obligations with regards to information governance. This includes the following disciplines: Data Protection, Freedom of Information, Environmental Regulations, Cyber Security, Transparency Code, and Records Management.

Contents

1 Introduction

This annual report, provided by the Barnet Council's Senior Information Risk Owner (SIRO), outlines the activities and performance related to information governance and provides assurance that all information related matters across the Council are being effectively managed. The report reflects on the work undertaken during the financial year ending 31st March 2023 and highlights the progress made; where improvements are required to ensure compliance with the legislation, and details the plans in place to minimise risk and improve performance. The council continues to be committed to effective information governance and the governance arrangements are closely monitored to ensure systems, policies and procedures are fit for purpose; and that all council staff, elected members and key partners understand the importance of information governance and security, comply with legislation, and adopt best practice.

The role of SIRO undertaken by the Executive Director of Assurance and is Deputised by the Head of Assurance and Business Development.

2 Key Roles and Responsibilities

Council Management Team

Chaired by the Chief Executive, the Council Management Team (CMT) is in place to provide overall management and leadership of the council and work with Members to set the strategic outcomes for the borough. It sets and monitors the future direction of the council and ensures high performance against outcomes. Representation is across all service delivery units at the highest level of management.

Key responsibilities relevant to accountability and assurance include:

- Ensure the statutory duties of the council are effectively discharged
- Ensure business continuity and disaster recovery plans are sufficiently robust
- Ensure effective decision making and an internal control environment
- Agree intervention approach when assurance is not satisfactory
- Review of the Corporate Risk Register including report of the Senior Information Risk Owner
- Manage escalated risk

SIRO

- The SIRO at the London Borough of Barnet has overall responsibility for the council's information risk and risk assessment processes. The SIRO is a member of the Council Senior Management Team and chairs the Security Board.
- They have responsibility for leading and fostering a culture that values, protects and uses information for effective delivery of the council services and functions.
- Their role is to focus on strategic information risks related to the delivery of the council's corporate objectives and taking into account the council's risk appetite to take a holistic approach to information risk across the council.

Deputy SIRO:

- Provides a focus for the management of information governance at a senior level

- Provides advice and reports in respect of information incidents and risks, including the content of the Council's Annual Governance Statement relating to information risk
- Owns the management of information governance and risk assessment processes within the Council
- Understands 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
- Chairs the council's Security Forum.

The Data Protection Officer:

- Provides independent advice, guidance and reports in respect of all aspects of information management
- Ensures the council's implementation of policies, standards and procedures for Information Governance aim to reduce the risk of legal action from individuals, organisations or regulators
- Responsible for creating and maintaining the council's statutory records of data processing activities and Data Sharing Agreements, ensuring the Council is not acting outside of its powers
- Acts as the primary 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
- Responsible for identifying key control failings / weaknesses in information management processes and provide support to senior managers to adopt new practices and procedures to improve operational performance and reduce risk.

The role of the statutory Data Protection Officer is held by the Records and Information Service Manager and has a dotted line of responsibility to the SIRO.

In addition to these key Officers, there are a number of statutory and non-statutory Officers across service areas offering support in relation to information governance and information security.

- **Records and Information Management Team** - this is the specialist corporate lead and resource for supporting and assuring the council's compliance with information law, and the effective management of council records and information at every point of its lifecycle, from its creation to its deletion/destruction or long-term preservation.
- **IT Security Manager -** the role of the security manager is to promote and adopt security best practice. Working with the organisation, IT operations, architectures validating best practice around security and recommend changes to enhance security posture and risks. Also works with key stakeholders to ensure the organisation is PSN and PCI compliant from a network perspective and the organisation meets ISO27001 requirements.
- **Legal Services -** Legal services are provided to the council by Harrow Barnet Public Law (HBPL). They support the SIRO in providing legal advice on contentious or high risk matters, that affect the council or its assets. Ensuring the council adheres to any legislative or regulatory requirements.
- **Link Officers and Records Champions (within delivery units)** - These officers work closely with the Records and Information Management Team acting as the point of contact for

information management related requests. Taking responsibility for dealing and responding in line with the relevant legislative requirements. They are responsible for promoting best practice within their service and adherence with council policy.

3 Governance and Monitoring arrangement

The SIRO is supported by the following Boards / Groups:

- **Security Board**

  The Security Board meets quarterly and is responsible for monitoring and making decisions on key risks associated with the security of the council, this includes, information security, physical security, building security, cyber security, and data protection. The Security Board is a point of escalation for serious security issues and reports directly to the Council Management Team. It is chaired by the SIRO.

- **Security operations Forum**

  The Security Operations Forum underpins the Security Board. It meets monthly and facilitates cross-area discussion on operational, day-to-day, issues relating to security and information management. The Forum tasks actions that will improve the security of Barnet Council with the aim to protect its staff, assets, information, and data. It is chaired by the Deputy SIRO.

- **Information Management Governance Groups (IMGGs)**

  IMGGs exist within the following areas of the council:

  - Barnet Education and Learning (BELS)
  - Family Services
  - Communities and Adults
  - Assurance

  Representatives from each delivery unit attend regular sessions (6 weekly) along with Lead Officers within the Council's Records and Information Management Team to discuss any emerging issues or concerns. The group are accountable for driving delivery of the organisation's Information Management objectives, ensuring information management compliance within their delivery unit and maintaining oversight of breaches and incidents, with a primary aim to improve information management compliance and reduce risk.

4 Risk Management

The council has in place a robust Risk Management Framework.

Risk Registers are held and regularly maintained and updated by all service areas. Risks, including Information Management risks, are logged, escalated and reviewed in line with the council's Risk Management Framework.

A copy of the current Information Management and Cyber risks are attached as Appendix A.

Risk Management Process

The council also has a number of risk and review processes in place to assist in assessing and mitigating information risk. These include:

Data Protection Impact Assessments:

This is a tool to help organisations identify the most effective way to comply with data protection obligations. They are used at project inception to ensure information risks are identified and dealt with early and also where new or changes to information sharing may result in high risks to data subjects.

There is a requirement built into policy that all new projects and processes are assessed for whether a statutory DPIA (Data Protection Impact Assessment) is required, and if not, a more informal IMIA (Information Management Impact Assessment) is completed.

All DPIA's are checked by the Council's Data Protection Officer.

No DPIA's have required a high risk referral to the Information Commissioner for 2022/2023.

Supplier / Service Provider Due Diligence:

As outlined in the Council's Procurement Toolkit, services must undertake information management due diligence with any new contractors or service providers, ahead of contract. A Due Diligence Template is in place for this purpose.

Contracts are required to contain standard approved data protection, FOI and Transparency contract clauses which ensure our service providers meet appropriate standards when undertaking work on behalf of the Council.

The London Office of Technology and Innovation (LOTI) is funding a project to review the due diligence processes used by all London boroughs. Barnet is active on the working group tasked with developing a standardised due diligence process that will result in six primary outputs:

- Cybersecurity Questions - to be answered by contractors.
- IG Questions - to be completed by contractors.
- Accreditations - a compendium of common accreditations (e.g., DSPT, ISO27001) and the aspects of IG and cyber that they address, along with the weight that should be assigned to them.
- Evidence - A list of documents a local authority (LA) expects a (proposed) contractor to provide, such as a DP Policy, ICO registration, or PSN certificate.
- Evaluation guidance - for IG officers, contract managers and procurement teams on how to evaluate questionnaires and evidence.
- Contract Monitoring & Audit - Guidance on what to evaluate in ongoing contract management and on how to handle SLA breaches or noncompliance.

The working group will recommend that all London boroughs use the standardised outputs in their own contracts, to provide greater assurance around the provisions on service providers and improve procurement practices and information management standards. This work should be completed in 2023/2024.

IT Approval Process:

All requests for IT Software or Systems are subject to a formal assessment and approval process. Each submitted request is reviewed by CSG IT from a technical, strategic and application support

perspective; by the LBB Business from a strategic perspective; and from the Records and Information Management Team from an Information Management and Data Protection risk perspective.

NOTE: Every process has an identified risk escalation path in place, where high risk risks are either referred to the DPO, the SIRO or where appropriate the Security Board.

5 Internal Audit

Internal Audit play a key role in assisting the SIRO, by working to ensure a positive culture of internal control, effective risk management and good governance.

The following Audits undertaken in 2022/2023 have relevance to Data Privacy and Information Security:

Audit Title	Date	Scope areas	Assurance Rating	Relevant findings
Cyber Security - Third Party Security and Awareness	March 2023	• Third-party cyber risk management for IT suppliers • Cyber security training and awareness	Limited	The Council has two complementary cyber security related training modules (Cyber Crime and Cyber Security) available to Council staff over the intranet. However, these training modules are not mandatory. The Council is, currently, considering an overhaul of the training programme. Escalations for incomplete training are automatically sent through emails to respective line managers. However, training completion was not found to be sufficiently enforced at the Council as staff training completion levels against specific due dates were not readily tracked. The Council has not identified high-risk roles within the organisation (such as privileged system users, administrators, senior officers etc.) that may require specific cyber security awareness education and training.
Recruitment - Pre-employment Checks	March 2023	• Policies and Procedures • Roles and Responsibilities • Staff Vetting	Limited	<u>One High risk finding: GDPR concerns</u> Per the GDPR policy set by the Council, only relevant personal information should be captured and held, and all personal data should be deleted ten years after an employee leaves the Council.

				We reviewed the process and noted the following: - Pre-employment documents are retained within shared folders on file explorer, which is not a safe or secure location. These files could potentially be accessed by anyone in Capita HR, and it was unclear whether the wider Capita team could also access such files. - All information received from the Council is stored, rather than only the information required to be retained. Management confirmed that all information received is stored and there is no mechanism to review and retain only what is required in line with regulation. - Both the Barnet Recruitment Team and Capita HR are working towards a six-year document retention period for pre-employment purposes, rather than the ten-year period defined by the 'big bucket' approach the Council have adopted. Documentation is consequently not deleted in line with guidance set out by the Council.
Remote Working	June 2022	• Policies and Procedures • Awareness, Communication and Training • Access Management • Data Loss	Reasonable	**<u>Restrictions on Cloud Applications (medium risk)</u> –** There is currently a lack of appropriate controls restricting third party cloud applications, which could result in confidential council data being leaked or accessed by inappropriate parties. The increasing endorsement of cloud-based 'software-as-a-service' (SaaS) applications that can be accessed online has made data sharing easier but has also heightened the risk of data loss. Management should review and risk-assess which cloud sharing platforms should be permitted and implement

				blacklisting rules on riskier cloud applications. **<u>Oversight of staff working overseas (medium risk)</u> –** The Council does not have sufficient guidance on and oversight of staff working overseas. We noted that the Council does not have a centralised register that tracks employees overseas. This reduces the level of oversight that the Council has to ensure that employees are adequately supported when working abroad. The Council should ensure Insurance receive the monthly report of staff who have applied to work overseas so that they have visibility of staff planning to work abroad, and issue guidance to staff and managers that sets out the Council's policy for overseas working. **<u>Lack of a Data Loss Prevention (DLP) strategy (low risk)</u> –** A Data Loss Prevention (DLP) strategy sets out how an organisation detects and prevents potential data breaches or data being inadvertently shared or transmitted. The Council does not currently have a DLP strategy. However, we did note that the Council currently has a number of controls in place to help mitigate the risk. It is important that the Council produces documentation that details the Council's approach to data loss prevention. **<u>Cyber Security information (low risk)</u> –** Due to the increased reliance placed on IT security practices due to the advent of remote working, it is important to regularly communicate and spread awareness of targeted methods of data theft such as phishing and malware attacks. We have seen that staff do not receive regular communications in relation to data/cyber security risks and

				issues, which may lead to an increased risk of cyber/data security breaches occurring.

6 Overview of Statutory Performance April 2022 – March 2023

6.1 Freedom of Information

Year	Requests Received	Percentage responded to within statutory deadline (Target of 95%)	Internal Reviews Received	Internal Reviews – original decision fully upheld	Complaints Received from the Information Commissioner	Decision Notices issued against LBB by the Information Commissioner
2020/2021	1882	96%	40 (2%)	19 (plus 4 upheld in part)	5	0
2021/2022	1556	97%	40 (3%)	14 (plus 13 upheld in part)	12	0
2022/2023	1622	96%	53 (3%)	22 (plus 12 upheld in part)	7	1

- FoI performance remains high across most services, and the council again exceeded targets.
- An "upheld" refers to the council's original decision. E.g. the review will full support withholding information and the original application of the exemptions applied.
- An "upheld in part" can refer to a variety of differing outcomes. E.g. the original decision to withhold is upheld as part of the review, but the application of exemptions in the original response has been found to be incorrect.
- Whilst the number of reviews received are high, it is encouraging that upheld and complaint figures demonstrate a robust review process as very few requests have resulted in an ICO Decision Notice overturning our response.
- The council is looking to introduce a programme of quality assurance measures to identify potential improvements to further reduce the rate of escalation to internal review stage.
- In October 2022/2023 we received one decision notice from ICO against the Council in relation to the application of the repeated request exemption. However, this decision did not result in the council being required to release any information that had previously been withheld.

6.2 Transparency

The FoI Act requires every public authority to have a publication scheme approved by the ICO and Barnet's scheme is available here: Home | Barnet Open Data

The council aims to not only meet the requirements of the Transparency Code of Practice but to exceed them. The following work has been completed in 2022/23:

- **Transparency Review** - we have worked to ensure that all datasets required under the Local Government Transparency Code, along with other priority datasets, are now up to date and will establish an ongoing monitoring and update process for all datasets. In 2023/24, this project will broaden its scope to look at reviewing all other statutory publication regimes that impact local authorities.
- **Historical Document Publication** - we have worked with Local Studies & Archives to publish historical documents, books, pictures and maps relating to the history of the area on the Open Barnet portal. This has enormous potential and has already received very positive feedback. Work will be ongoing to further improve and expand this resource.

The following work will be undertaken in 2023/2024.

- **Improve Transparency rights** - Updating of privacy notices, privacy information for specific service areas, data protection page, open data & information requests, emails, websites and cookies and complaints pages on our external facing website to ensure that the information provided is clear and easy for our residents and members of the public to access.
- **Information Rights Engagement** – We have established an action plan to ensure a public engagement approach across information rights, with the aim of developing a proactive framework in line with the ICO's own internal processes and best practice recommendations. Implementation of and expansion of this plan will begin in 2023/24.

6.3 Subject Access Requests

Under the Data Protection Act 2018, any living person has the right of access (commonly referred to as a Subject Access Request), which gives individuals the right to obtain a copy of their personal data.

The last 3 years performance data is as follows:

Year	Requests Received	Percentage responded to within statutory deadline	Internal Reviews Received	Internal Reviews Upheld	Complaints Received from the Information Commissioner	Decision Notices issued against LBB by the Information Commissioner
2020/2021	166	49% **Large backlog and staffing resource*	6	2 (plus 1 upheld in part)	10	0

Year	Requests Received	Percentage responded to within statutory deadline	Internal Reviews Received	Internal Reviews Upheld	Complaints Received from the Information Commissioner	Decision Notices issued against LBB by the Information Commissioner
		issues as a result of Covid deployment, led to increased delays				
2021/2022	223	86%	13	5 (plus 2 upheld in part)	3	0
2022/2023	205	95%	18	6 (plus 4 upheld in part)	6	0

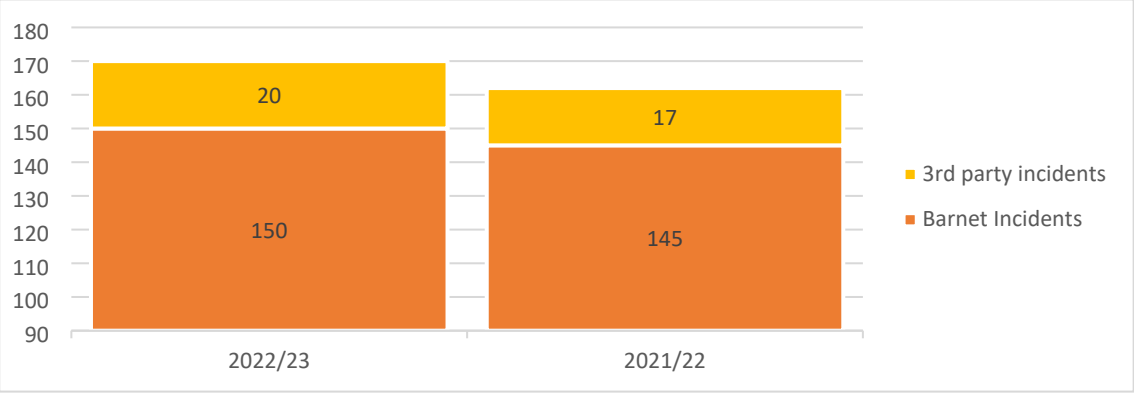
6.4 Data Protection Incidents

The council has an excellent culture of reporting incidents regardless of the nature or risk of the issue. Incidents can provide valuable insight into training, policy and process which may need to be strengthened as a preventative measure.

Not all incidents reported have resulted in a breach for Barnet.

Business continuity plans are regularly reviewed to respond to risks.

Number of incidents reported in 2022/2023 and 2021/22



Reporting Year	Number of Incidents Reported to the ICO	ICO Outcome
April 2022 – March 2023	2	No further action.
April 2021 – March 2022	3	No further action.

Breakdown of incidents reported for 2022-2023

The following categories are used within our incident reporting system, these categories and numbers of each potential breach are outlined below.

Category	Number
Disclosure – Email	59
Loss of equipment	23
Disclosure – Other	15
Disclosure – Intentional but inappropriate	10
Inappropriate security applied	10
Disclosure – Postal	8
Inappropriate / excessive processing	8
Inaccurate data / Loss of integrity	5
Disclosure – Verbal	4
Deliberate or wilful act	2
Loss of data	2
Technical / procedural fault	2
Unauthorised access	2
Destruction / Deletion of data	0
Insufficient privacy information	0
PECR (Privacy and Electronic Communications Regulations)	0

Every incident reported is given an initial risk rating based on the likelihood of harm occurring and the impact that harm may have on relevant affected individuals. The 150 Barnet managed incidents were rated as follows:

- 24 Incidents – No Risk
- 95 Incidents – Low Risk
- 31 Incidents – Medium Risk
- 0 Incidents – High Risk

Learning from breaches:

As part of the investigation process every incident is assessed and actions assigned to services, where required, to identify opportunities to reduce the chances of a similar breach occurring in the future. These may include issuing further training, a amendment of process or policy, or targeted internal communications to remind staff regarding correct process, or highlight a risk.

Patterns of incidents, or higher risk concerns are shared across the organisation through Information Management Governance Groups to remind them of good practice in avoiding breaches occurring.

6.5 E-Learning Training Completions

All staff are required to undertake mandatory Data Protection Essential and Information Security e-learning as part of their induction.

Staff are required to complete this training within 8 weeks of joining and to refresh the training every 12 months; they are sent reminders about the expiry date of their training, which are escalated to Line Managers if training is not completed.

Completions rates in June 2023 were as follows:

Service	DP Essentials	Info Security
Adults and Communities	86%	89%
Assurance	95%	95%
BELS	95%	96%
Customer & Place	93%	93%
Environment	90%	90%
Family Services	98%	97%
Public Health	98%	98%
Strategy & Resources	88%	88%
Street Scene	96%	96%
Council Total	**93%**	**94%**

The council seeks a 95% completion rate overall.

This requirement takes into account the fluctuation of staff absences, such as external secondment, long term sick, or maternity leave.

E-Learning Improvement Work

The council acknowledges that completion rates for training are lower than the 95% it aspires to achieve and work to improve the take up of the e-learning modules is underway.

Although completion targets have not been achieved, it should be noted that significant efforts have been made to promote and encourage engagement with the training and this will continue.

A report has been written to provide the following recommendations:

- **E-Learning Monitoring:** line managers to actively monitor and address completion of modules at onboarding / probation, 1 to 1's and supervision.

- **Data Accuracy:**
    - Managers should be reminded to adhere to established protocols for Starter, Leaver and mover processes. Providing relevant data in a timely manner to allow the system to be as accurate as possible.
    - Mechanisms need to be put in place to allow the validation of data for all service areas on a regular basis e.g. provision of lists of staff to managers to be checked and signed off.
    - The current HR Core system is due to be replaced with a new HR system called Oracle; therefore, we recommend that an establishment data cleanse is undertaken ahead of the transfer to Oracle.
    - The Oracle system must ensure that it a takes into account the feed to the POD system and testing should be undertaken to ensure the data is coming through correctly.

The above recommendations have been passed to Internal Audit to include as part of their own review of mandatory e-learning across the council.

7 Data Security and Protection Toolkit

Organisations that process and share NHS patient data are required to undertake an annual online self-assessment, referred to as the Data Security and Protection Toolkit.

The successful completion of the toolkit demonstrates assurance that good data security and governance monitoring is in place, and that personal information is being handled correctly.

The assessment was successfully completed and submitted in June 2023. There were no outstanding actions at the time of submission.

8 Records Management

The Council acknowledges that effective records management supports effective data governance, data protection and appropriate decision making.

This year the Council has embarked on a project to scan all of its property deeds. A new process will be introduced which will include creating digital copies of deeds which will be the primary records accessed on a day-to-day basis. The project will bring about improved access (speed and access control). The scanning process itself will mitigate the current risk of deterioration by ensuring that the original hardcopy records are only accessed and handled rarely. This will help to mitigate the currently risk of deterioration and help to preserve our original documentation for longer.

The project will also bring additional benefits such as reduction in delivery costs and reduction in duplication of paper records. Both of which will contribute to the council's drive for net zero.

We have also planned a full review of the records retention schedule and an audit of our off-site storage holdings. We will be looking at retention within systems, as well as electronic and paper records, and a review of processes. Internal audit will also be undertaking a records retention focused audit in the 3rd quarter of 2023. Any recommendations will feed into our review.

9 IT and Cyber Security

Cyber-attacks remain a high risk overall to the Council and the impact of a cyber security attack would be significant with most if not all services affected. Knowing the significance of this impact

the Council is continually strengthening security controls to minimise the likelihood of an external cyber-attack.

The Cyber Security threat landscape is actively monitored and working closely with National Cyber Security Centre (NCSC) any emerging threats or intelligence that are identified are mitigated. The Council continues to subscribe to appropriate cyber security network alert services.

All Council issued devices laptops and smartphone are encrypted to ensure the safety of Council data should the device be lost or stolen. The Council also has password phrase adding complexity in accessing Council devices and data.

Critical security patches are updated to ensure that all applications have the latest patches and hackers are not able to exploit these vulnerabilities. In addition, there is a robust patching regime in place for Windows updates.

Firewalls are managed and monitored to assist in the prevention of any dangerous programs, virus, or spyware before they can infiltrate the network.

The Council secured some funding from the Department of Levelling Up, Housing and Communities to support our cyber security protection.

During the year, the Council retained its PSN compliance certificate with any highlighted areas of improvement addressed and is also PCI compliant.

Phishing scams are the most common type of cyber-attack in the UK, accounting for 44% of all incidents. This is where the user inadvertently downloads software or allows access to networks. As part of improving training and awareness regular communications and phishing exercises are run to allow help users spot a phishing email to prevent a real attack.

Another key area that affects the Council is the attack on supply chain, this can be suppliers of applications or delivery of services to the council. When either themselves or one of their subcontractors is attacked by hackers, they also try to attack all the other organisations.

Several technical improvements were delivered during the year to enhance the Councils Cyber Security, some of which are:

- Enhanced monitoring of traffic and trends and blocking of suspicious traffic
- Moving to Microsoft E5 Licencing which includes enhanced security features.
- Close working with NCSC and other regional and national bodies on Cyber
- More robust change management for applications and the introduction of an approval process in the use or purchase of new software
- Monitoring of overseas working and ensuring all employees have approval.

Moving forward 2023/24 will see:

- Improvements and additions of cyber security to the information management training module
- Changes to include cyber security in the supply chain of services and applications.
- Introduction of data labelling

2022/23, also saw: 543 changes made to either applications or to the network.

To date 23/24: we have had 492 changes made to either applications or the network.

10 Policy Reviews

The council's Records and Information Management Team maintains and review a comprehensive suite of policies, standards, toolkits and procedures. These are subject to regular review and update.

Of the 21 policies and standards in existence, 12 of these received review in 2022/2023, 3 are due review in March 2024, and the remaining 6 will be reviewed in 2023/2024.

APPENDIX A – Information Management Risks

Risk Description	Controls and Mitigations in Place	Residual Risk - Total	Response Option	Treatment Actions	Direction of Travel (from previous quarter)
Non-compliance with data protection legislation including GDPR - Council staff and partners failing to follow GDPR legislation, including the organisation's policy and processes, could lead to data protection breaches resulting in enforcement action and monetary fines, complaints, adverse impact on individuals and claims for compensation.	1. Information Management's framework of policies, and a specific data protection toolkit controls is published and regularly reviewed 2. All staff receive e-learning (including at induction) and follow up training offered in more sensitive areas 3. There is effective incident management, and Information Management Governance Groups 4. Council wide Security Board meets quarterly, chair by the SIRO and Security Operations Forum, meets monthly, chaired by the deputy SIRO 5. Key contacts within the council have been receiving guidance 6. Ongoing communications to council staff on information management guidance 7. E-learning reminder to all staff, included in initial induction pack for new starters 8. 6-monthly reporting to CMT for discussion and review.	12	Treat	1. Refresh of records and information management policy suite 2. Further communications and engagement with services to ensure the completion of the mandatory e-learning modules.	Reduced
Records not destroyed in line with legislation (retention) Directorates not destroying information in a timely manner once the information has reached its retention date and is no longer required to be retained by the council could lead to data breaches resulting in enforcement action.	1. Destruction reminders at Information Management Governance Group (IMGG) 2. Continuous development of Barnet's Retention Schedule to include more files types to improve accuracy in retention date allocation 3. Reports are generated by Records Management every six months on offsite stored files which have reached their assigned retention period - these are circulated for review to Records Champions and escalated at IMGG if applicable.	12	Treat	1. Support service areas in reviewing the backlog of overdue destruction reviews and documents held. 2. Review and re-training of Records Champions in late 2023, early 2024 to ensure knowledge is	

Risk Description	Controls and Mitigations in Place	Residual Risk - Total	Response Option	Treatment Actions	Direction of Travel (from previous quarter)
	4. Outstanding files are reviewed, monitored and escalated at Security Board.			retained and expanded across the organisation and that officers are aware of their duties within this role. 3. Re-education and sessions around the use of Email, MS Teams and other Council software to ensure information is being stored and processed in line with Records Management Policies and procedures 4. Records Destruction Audit beginning in October within Customer and Place, this will enable us to pick up on good practice as well as highlight recommendations for improvements that can be replicated across other service areas.	

Risk Description	Controls and Mitigations in Place	Residual Risk - Total	Response Option	Treatment Actions	Direction of Travel (from previous quarter)
Confidential waste not destroyed - Confidential waste not being securely destroyed or overfilled confidential bins could lead to data breaches resulting in enforcement action.	1. Confidential Waste is managed by the Facilities Management team through the use of shredders at print points and confidential waste consoles have been installed on 6th, 7th and Ground floors in Colindale 2. Regular office walk-arounds by Records Management 3. Guidance issued to staff regarding working from home protocols re. printing and confidential waste.	9	Tolerate	There are no further actions at this time. The risk has reached its target score and is being tolerated with the existing controls and mitigations in place.	
Loss / damage of physical records - Documents not stored in relation to retention policy (improper use of storage, poor records management) or damage to the building (fire, flood, restricted access) could lead to records being damaged or being inaccessible resulting in loss or destroyed of confidential, statutory or highly valuable information such as property deeds and financial impact to the council.	1. Appropriate building regulations being followed 2. Policies and procedures in place on guidance on proper records management processes - continuous education and communication of best practice through Information Management Governance Group (IMGG) occur regularly.	9	Treat	1. 1. Deeds Scanning Project underway August 2023 to ensure the risk of paper records is mitigated.	

Risk Description	Controls and Mitigations in Place	Residual Risk - Total	Response Option	Treatment Actions	Direction of Travel (from previous quarter)
IT cyber security - A cyber attack could lead to the council being unable to operate resulting in widescale disruption and financial cost.	1. There are multiple-layer firewalls to protect the environment. 2. Annual Security Health Check (Public Sector Network (PSN) Standard). 3. PCI Accreditation. 4. Annual review of over 100 cyber security controls, aligned with ISO 27001. 5. Anti-virus on the server estate. 7. Subscribe to National Cyber Security Centre (NCSC) early warning system and web check. 8. Receive weekly updates from NCSC to confirm vulnerability status. 9. Receive weekly and critical updates from Microsoft/ Capita. 10. Annual Cyber Security training and awareness for staff. 11. 24hr Emergency Response 12. Microsoft E5 security - including: advanced threat protection (ATP), advanced threat endpoint protection ATEP 13. Safelinks - email URL scanning to protect access to malicious links that are used in phishing and other attacks. 14. Additional cyber security audit with PwC completed, action plan created. 15. Worked with Business Continuity leads to improve plans to manage impact. 16. Applied for and received funding from DLUHC, with action plan linked to funding. 17. The implementation of an online web protection application (Imperva) preventing DDOS attacks specifically for the Barnet websites	15	Treat	1. Develop additional scenario based training to roll out to senior staff (funding provided by London Councils). 2. Implement action plan from PwC audit to be completed. 3. Implement action plan from BC review. 4. Implement action plan tied to DLUHC funding.	Same

Risk Description	Controls and Mitigations in Place	Residual Risk - Total	Response Option	Treatment Actions	Direction of Travel (from previous quarter)
Cyber security - A cyber attack could lead to the council being unable to operate resulting in widescale disruption and financial cost.	1. Monthly contract management meetings in place to manage the contract and relationship with CSG. 2. Monthly Partnership Operations Board for escalation of any issues identified. 3. Joint risk being managed by CSG - IT with controls/mitigations in place. 4. Learning portal - mandatory training on Information Management/cyber security for staff. 5. Regular audits undertaken. 6. PCI (payment card industry) accreditation. 7. Management and oversight of the actions being carried out by CSG on the council's behalf (captured in the joint risk register). 8. BC leads have provided plans in case of a cyber security event. 9. Remote working audit completed and recommendations implemented on working abroad policy and external websites. 10. Simulated phish went to all staff, and recommendations implemented. 11. PwC audit completed on supply chain. 12. Implemented website health recommendations. 13. Microsoft 365 health check completed and recommendations implemented including updating password rules.	15	Treat	1. Spend money on enhanced training through Barnet's Learning Management System (or POD - Place of Development). 2. Promote information and security training. 3. Implement with business continuity lead action plan. 4. Implement recommendations from PwC audit on supply chain risk.	Same