Governance, Audit, Risk Management and Standards Committee

Title	Senior Information Risk Owner (SIRO) Annual Report 2022 - 2023
Date of meeting	18 January 2024
Report of	Clair Green, Executive Director of Assurance
Wards	All
Status	Public
Urgent	No
Appendices	Appendix A - Senior Information Risk Owner (SIRO) Annual Report 2022 - 2023
Officer Contact Details	**Clair Green,** Executive Director of Assurance Clair.green@barnet.gov.uk **Emily Bowler,** Assistant Director of Assurance emily.bowler@barnet.gov.uk **Ali Saka,** Head of Assurance and Business Development ali.saka@barnet.gov.uk

Summary

- This report presents a summary of information governance risks, issues, and the council's activities to ensure appropriate governance of information within the Council.
- This report provides assurance to the Committee that the council's information governance policy and practice is in line with legal obligations and consistent with the principles of good governance.

Recommendation

That Committee:

1. note the council's activities and position in respect of information risk as set out in the report
2. consider any further steps it may wish to see taken to promote good practice in information governance within the Council

1. Reasons for the Recommendations

1.1 Production of an Annual SIRO Report is seen as good practice that is being introduced by growing number of local authorities.

1.2 This report is presented with the intention to support the Committee in discharging its responsibilities in relation to corporate governance, which includes information governance.

1.3 This report covers the reporting period 1 April 2022 - 31 March 2023 and provides assurance of compliance with regards to the council's information governance obligations.

1.4 The council's information governance arrangements are closely monitored by relevant management teams and governance boards 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.

1.5 The council has designated information management roles which include Data Protection Officer, SIRO, and Caldicott Guardian.

1.6 Information Management risks are identified, logged, escalated, and reviewed in line with the council's robust Risk Management Framework.

1.7 Data protection impact assessments are used to assess data impacts of all projects and major processes

1.8 Information management due diligence of suppliers and IT approval processes use escalation paths to ensure there are appropriate risk assessment and governance arrangements concerning information risks.

1.9 The internal audit service conducts audits that support the council in maintaining a positive information management culture, governance, and internal controls. The audits carried out during the reporting period focussed on third-party cyber risks, staff cyber security training, pre-employment checks, and remote working; recommendations from each audit have been actioned.

1.10 The council has a robust process to review and respond to Freedom of Information (FoI) requests and continues to exceed its target which is 95%.

1.11 The council continues to exceed the recommendations of the Transparency Code of Practice; the council's proactive approach to transparency reduces the demand on its resources to respond to higher number of FoI requests.

1.12 Despite the council receiving increasing number of subject access requests, it continues to show year-on-year improvement in timelines of responses (95% in 2022/2023)

1.13 The council has a positive culture of reporting information incidents; lessons from incidents are used to improve processes and shared across the council to maintain awareness.

1.14 During the reporting period 150 incidents involving council services and 20 incidents involving third parties were reported; none were rated high risk and 2 incidents required ICO reporting (both resulted in no further action).

1.15 All staff are required to undertake mandatory Data Protection Essential and Information Security e-learning; the council has achieved the 95% target for training compliance and published its Data Security and Protection assessment. Mandatory training compliance is an area of current focus to improve ongoing compliance, associated processes, and data quality.

1.16 The council has continued to reduce its offsite storage holding through improved retention reviews and digitalisation of records. These deliver cost savings and support the council's drive to net zero.

Cyber-attacks remain a high risk and the council is continually strengthening security controls to minimise the likelihood of a cyber-attack. This includes active monitoring of threats, communication traffic and information flow; intelligence sharing; improved change management and IT approval processes, physical and digital security controls put in place to safeguard council devices and IT estate, as well as its supply chain.

In 2023/2024 will focus on improving staff training, cyber security of the council's supply chain, and data labelling.

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

1.18 All information management risks are reported as part of the quarterly strategic risk updates and each risk is routinely reviewed, and appropriate measures implemented to treat/reduce its risk/impact. Potential impact of a cyber attack remains high as it could impact the council's ability to operate or result in widescale disruption and financial cost. Various controls and business continuity measures are implemented to mitigate and respond to a potential attack.

2. Alternative Options Considered and Not Recommended

2.1 The Senior Information Risk Owner (SIRO) Annual Report is considered by the council's senior officers.

2.2 The Committee may choose to exclude the report from future committee meetings. The Governance, Audit, Risk Management and Standards Committee's consideration of this report supports the council's commitment to good governance and transparency.

3. Post Decision Implementation

3.1 None

4. Corporate Priorities, Performance and Other Considerations

Corporate Plan

4.1 Good information governance and transparency ensures the council remains compliant and engaged, which support the delivery of the Council's vision as set out in Our Plan for Barnet 2023-2026.

Corporate Performance / Outcome Measures

4.2 The Assurance Directorate Outcomes Framework is the means through which we provide assurance that the directorate works towards delivering the Council's priorities as set out in Our Plan for Barnet. Continuous improvement of information governance is a key priority for the council and ongoing compliance with information governance policies and procedures are monitored through the Assurance Outcomes Framework.

Sustainability

4.3 There are no sustainability implications arising from this report.

Corporate Parenting

4.4 There are no corporate parenting implications arising from this report.

Risk Management

4.5 The council has an established approach to risk management, which is set out in the Risk Management Framework. High level information governance and security risk are included within the quarterly strategic risk reports considered the Governance, Audit, Risk Management and Standards Committee.

Insight

4.6 Horizon scanning and learning from information incidents provides insight in relation to the council's information governance culture and current and future risks, and helps identify continuous improvement opportunities.

Social Value

4.7 There are no direct impacts on sustainability from noting the recommendations.

5. Resource Implications (Finance and Value for Money, Procurement, Staffing, IT and Property)

5.1 It is anticipated that all activity set out in this report is achievable within existing and planned budgets.

6. Legal Implications and Constitution References

6.1 Information governance is governed by UK legislation, regulation, statutory guidance, and case law. This report sets out, at a high level, the reasonable technical and organisational measures that the council is taking and plans to take in order to ensure compliance with this legal framework and minimise information risk.

6.2 The Council's Constitution (Part 2B) sets out the terms of reference for Committees. The responsibilities for the Governance, Audit, Risk Management and Standards (GARMS) Committee include providing "independent assurance to the members of the adequacy of Barnet Council's governance, risk management and control frameworks and oversees the financial reporting and annual governance processes. ".

7. Consultation

7.1 None

8. Equalities and Diversity

8.1 Decision makers should have due regard to the Public Sector Equality Duty in making their decisions. The equalities duties are continuing duties and not duties to secure a particular outcome. Consideration of the duties should precede the decision. It is important that Cabinet has regard to the statutory grounds of the Public Sector Equality Duty, which are found at section 149 of the Equality Act 2010 and are as follows:

A public authority must, in the exercise of its functions, have due regard to the need to:

- Eliminate discrimination, harassment, victimisation, and any other conduct that is prohibited by or under this Act;
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it;

- Having due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to:
  - remove or minimise disadvantages suffered by persons who share a relevant protected characteristic that are connected to that characteristic;
  - take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it;
- Encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.
- The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons' disabilities.
- Having due regard to the need to foster good relations between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to:
  - Tackle prejudice, and
  - Promote understanding.

8.2 Compliance with the duties in this section may involve treating some persons more favourably than others; but that is not to be taken as permitting conduct that would otherwise be prohibited by or under this Act. The relevant protected characteristics are:

- Age
- Disability
- Gender reassignment
- Pregnancy and maternity
- Race
- Religion or belief
- Sex
- Sexual orientation
- Marriage and Civil partnership

An equality impact assessment has not been completed for this matter. However, the Council has considered the equality implications of its communications systems, including the need to ensure that communication meets the need of a wider range of the public, including those with disabilities or neurodiversity, as well as those who may have a language barrier.

9. Background Papers

- Appendix A - Senior Information Risk Owner (SIRO) Annual Report 2022 - 2023