

North Lanarkshire Council Report

Finance and Resources Committee

Does this report require to be approved? Yes No

Ref REB/CC Date 04/03/26

Annual Data Protection Compliance and Activity Report for Financial Year 2024/2025

From Rachel Blair, Chief Officer (Legal and Democratic)

E-mail BlairR@northlan.gov.uk **Telephone**

Executive Summary

This report provides a comprehensive and strategic assessment of North Lanarkshire Council's performance and compliance with its statutory data protection and information governance obligations during the financial year 2024/25. It presents a detailed analysis of personal data breaches, engagement with the Information Commissioner's Office (ICO), Subject Access Request (SAR) performance, staff training and awareness, and the effectiveness of governance and assurance arrangements. The report fulfils the requirement for the Data Protection Officer (DPO) to report and provides assurance on the Council's overall compliance position.

Overall, the Council has demonstrated measurable and sustained improvement across several key areas of compliance. In particular, notable progress has been achieved in the management and governance of SARs within Social Work services, the development and delivery of targeted, service-specific training, and a significant increase in completion rates for mandatory data protection and information security training. These improvements reflect strengthened leadership oversight, clearer accountability, and increased organisational focus on information governance as a core corporate responsibility.

Notwithstanding this progress, the report also identifies areas where further improvement is required to ensure full and consistent compliance with statutory requirements and regulatory expectations. Increased scrutiny from the ICO, particularly in relation to SAR performance, underscores the need for continued focus on timely and high-quality responses, improved recording and tracking arrangements, and sustained staff awareness to prevent avoidable personal data breaches. A clear programme of ongoing and planned improvement actions is therefore set out to address these risks and to support continuous improvement.

The report also provides strategic insight into emerging legislative frameworks, technological enablers, and organisational trends that will influence the Council's information governance practices over the next three to five years. By integrating these insights, the Council can proactively manage regulatory change, optimise operational efficiency, and strengthen trust with residents, partners, and regulators.

Recommendations

It is recommended that Finance and Resources Committee:

- (1) Acknowledge the Council's data protection and information governance performance during 2024/25, including improvements achieved and areas requiring further development;
- (2) Acknowledge the statutory roles, responsibilities, and assurance provided by the Senior Information Risk Owner (SIRO) and the Data Protection Officer (DPO);
- (3) Acknowledges the ongoing and planned improvement actions, including:
 - a. Strengthened breach reporting and incident response processes;
 - b. Continued emphasis on mandatory training and staff awareness across all Council services;
 - c. Updated and enhanced policies, guidance and internal awareness campaigns;
 - d. Targeted training and support in higher-risk Service areas; and
 - e. Enhanced monitoring, reporting and senior oversight of SAR performance.
- (4) Acknowledge the incorporation of forward-looking, evidence-based strategies to anticipate and adapt to evolving regulatory requirements, technological innovations, and emerging data governance risks;
- (5) Acknowledge further development and refinement of information governance processes, including reviewing performance indicators, enhancing Schedule 2 request management, improving Data Protection Impact Assessments and Data Sharing Agreements, providing targeted training, updating guidance materials, and ensuring ongoing staff support; and
- (6) Acknowledge that information governance improvement remains a corporate priority and is embedded within service planning, digital transformation, and risk management arrangements.

The Plan for North Lanarkshire

Priority	All priorities
Ambition statement	All ambition statements
Programme of Work	Statutory / corporate / service requirement

1. Background

- 1.1 As a public authority and data controller, North Lanarkshire Council is subject to a comprehensive statutory framework governing the processing of personal data. Effective data protection and information governance are fundamental to maintaining public confidence, safeguarding individuals' rights, and ensuring compliance with statutory obligations, including the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). This legislation imposes enhanced accountability obligations, requiring the Council not only to comply with legal requirements but to be able to demonstrate that compliance through effective governance, documentation, and assurance.
- 1.2 Regulatory expectations, particularly those articulated by the ICO, have increasingly emphasised leadership accountability, evidence-based decision-making, and demonstrable continuous improvement. This report reflects that context and provides an integrated view of performance, risk, and assurance across the Council's information governance landscape.
- 1.3 During 2024/25, the Council has continued to strengthen its arrangements across the following core areas:
- Management and reporting of personal data breaches;
 - Engagement and compliance with the Information Commissioner's Office (ICO);
 - Delivery of mandatory and targeted staff training;
 - Compliance with individuals' information rights, particularly SARs; and
 - Strengthening governance, assurance, and accountability structures.
- 1.4 A strategic focus has been placed on anticipating emerging risks, embedding a culture of accountability, and ensuring that operational practices are both proactive and resilient to future regulatory developments. The Council has also sought to integrate technological solutions, including SAR tracking systems and secure communication platforms, to enhance efficiency and reduce human error.

2. Report

- 2.1 Robust governance arrangements are in place to provide strategic leadership, operational oversight, and assurance in relation to information governance and data protection compliance:
- 2.1.1 The Senior Risk Owner (SIRO) provides strategic leadership on information governance and information risk management across the Council, ensuring that information risks are identified, understood, and managed in line with the Council's risk appetite and statutory obligations. During 2024/25, the SIRO role was undertaken by the Chief Officer (Business and Digital);
- 2.1.2 The Data Protection Officer is responsible for overseeing compliance with data protection legislation, including the UK GDPR and the Data Protection Act 2018, providing independent advice to the Council, monitoring internal compliance, advising on Data Protection Impact Assessments (DPIAs), and acting as the primary point of contact with the Information Commissioner's Office (ICO). During 2024/25, the DPO role was undertaken by the Chief Officer (Legal and Democratic);

- 2.1.3 The Data Governance Board (DGB) provides strategic oversight of data protection and information governance, with regular reporting to the Business and Corporate Management Teams. It is responsible for setting direction, overseeing implementation, and securing assurance that effective arrangements are in place across the Council and its Arm's Length External Organisations; and
- 2.1.4 The Data Management Team supports the DGB by providing operational oversight, monitoring compliance, and driving day-to-day implementation and improvement.
- 2.2 The Information Governance Team within Legal and Democratic Services provides specialist legal advice and support across a wide range of information governance legislation, ensuring that services are supported to meet their statutory obligations. Through a combination of strategic oversight, operational monitoring, and continuous engagement with services, the Council ensures that its approach to data protection is integrated, proactive, and aligned with best practice.

Personal Data Breaches

- 2.3 A personal data breach is defined as a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes situations where personal data is made temporarily or permanently unavailable, where such unavailability is likely to have a significant adverse effect on individuals.
- 2.4 Where a personal data breach occurs, the Council is required to assess the likelihood and severity of any resulting risk to individuals' rights and freedoms. Where the assessment concludes that a risk is likely, the Council must notify the Information Commissioner's Office (ICO). Where a breach does not meet the reporting threshold, the Council is required to clearly document the rationale for that decision in accordance with the accountability principle under UK GDPR.
- 2.5 In circumstances where a breach is assessed as likely to result in a *high* risk to the rights and freedoms of affected individuals, UK GDPR requires the Council to inform those individuals directly and without undue delay. This assessment considers both the potential severity of impact and the likelihood of harm occurring. Timely notification enables individuals to take appropriate steps to protect themselves and mitigate potential adverse consequences.
- 2.6 During the financial year 2024/2025, the Council recorded a total of 102 personal data breaches, representing a significant reduction from 152 breaches in the previous financial year (2023/2024). Of these, six breaches met the threshold for reporting to the ICO, compared with ten in the previous year. This reduction reflects improving staff awareness, strengthened controls, and targeted preventative measures.
- 2.7 Table 1 below provides a service-level breakdown of recorded personal data breaches during 2024/2025, together with incidents classified as near misses. In line with ICO guidance, a near miss is defined as an incident that had the potential to result in a personal data breach but was successfully prevented.

Table 1

Service	Number of Breaches	Number of Near Misses	Reported to ICO	Reported to ICO within 72 hrs	Report to legal within 24
Adult Health & Social Care	19	2	2	0	13
Chief Executive's Office	22	0	1	1	13
Education & Families	44	0	2	1	33
Enterprise & Communities	17	1	1	1	12
Total	102	3	6	3	71

2.8 Personal data breaches that meet the statutory reporting threshold must be notified to the ICO within 72 hours of the Council becoming aware of the breach. To support compliance with this requirement, the Council operates an internal target whereby services are required to notify the Information Governance Team within 24 hours of becoming aware of an incident, even where only preliminary information is available. During 2024/2025, 71 of the 102 breaches were reported to the Information Governance Team within the 24-hour internal target. Of the six breaches requiring notification to the ICO, three were reported within the statutory 72-hour timeframe.

2.9 The remaining 96 breaches did not meet the threshold for notification to the ICO. The reasons for this are summarised in Table 2 below and reflect circumstances where the risk to individuals was assessed as low, such as successful recall or deletion of information, disclosure to trusted third parties bound by confidentiality, or limited personal data exposure.

Table 2

Service	Trusted third party (bound by confidentiality terms e.g. existing employee, Solicitor is the recipient) Includes recall, deletion or retrieved	Recipient Retrieval of document(s) or document(s) destroyed (no special category data)	Information disclosed contained Limited personal data	Email confirmed deletion	Process/System Error rectified	Passage of time low risk
Adult Health & Social Care	10	3	1	3		
Chief Executive's Office	7	1	3	8	2	
Education & Families	10	14	1	15	1	1
Enterprise & Communities	7	3	3	2		1

- 2.10 Of the six breaches reported to the ICO, three were not notified within the statutory 72-hour timeframe. Two delays were attributable to delays at service level, while the third occurred prior to June 2024, at which time the breach reporting form did not require the reason for delay to be recorded and, as a result, no information is held as to the reason for that delay.
- 2.11 To address this, the Council updated its breach notification form in June 2024 to require services to record reasons for any delay in reporting to Legal and Democratic Services and the ICO. This change strengthens accountability, improves auditability, and supports targeted improvement activity.
- 2.12 While compliance with the statutory reporting requirement has improved compared to earlier years, performance during 2024/2025 shows some inconsistency. During 2022/2023, 70% of reportable breaches were notified within 72 hours. This improved to 100% in 2023/2024. In 2024/2025, 86% of breaches were reported to Legal and Democratic Services within 72 hours, indicating a need for renewed focus on timely escalation. Prompt notification remains critical to enabling effective investigation, mitigation, and regulatory compliance.
- 2.13 Analysis of the Data Breach Register identified 31 breaches that were reported to Legal and Democratic Services outside the 24-hour internal target. In several early cases, the previous version of the breach notification form was used, which did not capture reasons for delay. The revised form now addresses this gap.
- 2.14 Reasons cited by services for delays in reporting breaches within the 24-hour internal target include:
- School holidays, public holidays, and service closures;
 - Delays in identifying or confirming a breach pending management input;
 - Incidents occurring close to weekends; and
 - Staff absence.
- 2.15 These factors highlight the importance of ensuring resilience within Services. Where a manager is unavailable, staff should escalate suspected breaches to an alternative manager or directly to Legal and Democratic Services, rather than awaiting a manager's return. The revised breach notification form now requires services to identify an alternative contact to support timely escalation.
- 2.16 The ICO did not take enforcement action in relation to any of the breaches reported by the Council during 2024/2025. It is noted, however, that the ICO's revised regulatory approach, introduced in June 2022 to reduce the financial impact of fines on public sector bodies and emphasise engagement and learning, concluded in June 2024. During the period of the revised approach, the ICO made increased use of alternative regulatory tools, including warnings, reprimands, and enforcement notices. With the conclusion of this approach, the likelihood of formal enforcement action, including financial penalties, may increase, reinforcing the importance of continued compliance and improvement.
- 2.17 Where the ICO provided recommendations following reported breaches, these were communicated to the relevant Services and supported by guidance from the Information Governance Team to ensure implementation and learning. Following each breach or near miss, the Information Governance Team works with the relevant service to identify root causes and implement preventative measures. Learning is shared at team, service, or corporate level, as appropriate, to support continuous improvement.

- 2.18 Analysis confirms that the majority of personal data breaches arise from human error, such as misdirected correspondence, incorrect attachments, or failure to update contact details. These risks are mitigated through improved staff vigilance, clear processes, and targeted controls. Following issues identified with the introduction of the Paris Delivery mail system, a cross-Service working group was established to strengthen controls. This included additional staff training and the requirement for Senior Officer checks prior to dispatch. The Council has introduced the Egress secure email solution to reduce the risk of email-related breaches. This system prompts users to verify recipients and attachments before sending, providing an additional safeguard against human error.
- 2.19 Guidance has been issued to schools and nurseries to prepopulate annual data check forms, reducing the risk of misdirected information. Some establishments have adopted additional visual controls, such as coloured paper, to reinforce awareness. To address risks associated with outdated pupil emergency contact details, schools have been reminded to verify emergency contact information for all pupils, with particular focus on those transferring between schools.
- 2.20 The Information Governance Team continues to work collaboratively with services following breaches to agree proportionate and practical preventative measures, embedding learning into operational practice. Mandatory data protection training, together with targeted sessions delivered by the Information Governance Team, remains a critical control in reducing breach risk. Increased training uptake during the reporting period is expected to contribute to a continued reduction in avoidable breaches across the Council.

ICO Complaints

- 2.21 Eight complaints were recorded with the ICO during 2024/25, an increase on previous years. The majority related to dissatisfaction with SAR handling rather than data breaches. Detailed analysis indicates that this was influenced by operational challenges, such as resource constraints, file accessibility issues, and lack of clarity on ownership of requests.
- 2.22 These insights have directly informed the Council's SAR improvement programme, including process redesign, targeted training, and improved record-keeping, thereby reducing the likelihood of future complaints and enhancing public confidence in the Council's data handling practices.

Training and Awareness

- 2.23 Completion rates for mandatory data protection and information security training increased significantly during 2024/25, with most modules now achieving completion rates close to or exceeding 85%. This increase demonstrates a positive cultural shift and greater staff engagement in their responsibilities for information governance.
- 2.24 In addition, the development and delivery of targeted SAR training for Social Work and other priority Services has strengthened staff capability and confidence in managing complex requests. The use of service-specific scenarios and practical exercises has been critical in translating legislative requirements into operational practice, ensuring consistent, high-quality responses.

Subject Access Requests (SARs)

- 2.25 Since April 2023, the ICO has required local authorities to submit regular statistical data on Subject Access Request (SAR) compliance. Analysis of this data has informed a targeted regulatory approach, with the ICO prioritising closer monitoring and engagement with authorities whose SAR closure compliance falls below 75%. The ICO’s stated expectation is that SAR compliance should consistently meet or exceed 90%.
- 2.26 During the financial year 2024/2025, the Council received 494 SARs, representing an increase on the 465 requests received in 2023/24. A detailed breakdown of SAR volumes and compliance performance is provided in Tables 3, 4, and 5 below.

Table 3 SARs for Financial Year 2024/2025:

Service	No of SARs	SARs responded to on time	% responded to on time
Social Work	314	234	75%
Non-Social Work	180	125	69%
Total	494	359	72%

Table 4 SARs for Financial Year 2023/2024

Service	No of SARs	SARs responded to on time	% responded to on time
Social Work	305	114	50%
Non-Social Work	160	80	83%
Total	465	194	60%

Table 5 SARs for Financial Year 2022/2023:

Service	No of SARs	SARs responded to on time	% responded to on time
Social Work	126	52	41%
Non-Social Work	84	68	80%
Total	209	120	57%

- 2.27 Overall compliance with statutory response times improved to 72%, compared with 60% in the previous year. While this represents meaningful progress, particularly in the context of increased demand, performance remains below the ICO’s expected benchmark of 90%, and further improvement is required to fully mitigate regulatory risk and ensure individuals’ information rights are upheld.
- 2.28 Significant improvement actions have been implemented, including strengthened governance, clearer ownership, improved access to records, targeted training, and enhanced monitoring and reporting. Early indications show these actions are having a positive impact, particularly within Social Work services.
- 2.29 Ongoing system enhancements, such as migration to Microsoft Teams for record tracking, integration with AI-enabled tools, and real-time dashboards via Power BI, provide the Council with deeper insights into workflow efficiency, risk exposure, and

operational bottlenecks. These measures allow proactive intervention and continuous performance improvement.

DPIAs, Data Sharing and Schedule 2 Requests

- 2.30 Data Protection Impact Assessments (DPIAs) and lawful data sharing arrangements are critical preventative controls. Progress has been made in embedding DPIAs within project governance, though further improvement is required to ensure consistent application at service level.
- 2.31 The Council has also strengthened oversight of Schedule 2 requests, primarily from Police Scotland, ensuring that disclosures are lawful, proportionate, and appropriately documented. This aligns with ICO expectations around transparency and accountability in data sharing.
- 2.32 Ongoing work to review and refine Data Sharing Agreements will further strengthen assurance and reduce risk.

Legislative Developments – The Data Use and Access Act 2025

- 2.33 The Data Use and Access Act 2025 introduces significant amendments to the UK data protection framework. While it does not replace existing legislation, it introduces new lawful bases, clarifies SAR obligations, strengthens complaint handling requirements, and updates international data transfer rules.
- 2.34 The Council will undertake a structured review of policies, processes, and guidance to ensure timely compliance as provisions of the Act are coming into force between 2025 and 2026. The Information Governance Team will continue to provide advice, training, and updates to services as further guidance is issued.
- 2.35 This legislation provides both opportunity and challenge, requiring strategic planning to integrate new compliance obligations into existing operational processes while enhancing transparency, accountability, and public confidence.

Strategic Insights and Forward Planning

- 2.36 The Council's data protection agenda is increasingly aligned with broader strategic objectives, including digital transformation, AI-enabled service delivery, and evidence-based decision-making. By leveraging robust governance structures, technological solutions, and targeted staff development, the Council is well-positioned to anticipate future regulatory requirements, mitigate emerging risks, and maximise organisational efficiency.
- 2.37 Key forward-looking considerations include:
- Embedding AI-assisted SAR processing to improve accuracy and reduce response times;
 - Continuous monitoring of DUAA implementation and alignment with ICO guidance;
 - Integration of data protection considerations into all digital service design and transformation projects;
 - Enhancement of cross-service data governance awareness and accountability;
 - Ongoing evaluation of risk exposure, breach trends, and staff capability to inform strategic resourcing decisions;

- Systematic review and refinement of key performance indicators to ensure they accurately reflect compliance and operational effectiveness;
- Strengthening processes for Schedule 2 requests, ensuring statutory criteria are consistently met and that monitoring and escalation processes are robust;
- Continued focus on completing Data Protection Impact Assessments (DPIAs) for all high-risk processing activities, with integration into project planning and risk management frameworks;
- Enhancing guidance and support materials, including scenario-based resources and targeted communications to embed best practice; and
- Expanding tailored training programmes to cover emerging areas of risk, legislative change, and evolving technology solutions.

Conclusion

2.38 The Council has made substantial and demonstrable progress in strengthening its data protection and information governance arrangements during 2024/25. Improved governance, increased training uptake, and targeted operational interventions have delivered measurable improvements in compliance and performance.

2.39 However, ongoing challenges remain, particularly in relation to SAR compliance, consistent breach reporting, and proactive management of emerging regulatory and operational risks. Sustained senior leadership oversight, continued investment in staff capability, technological enhancements, and process improvements will be essential to maintaining momentum, meeting regulatory expectations, and protecting the rights of individuals.

2.40 By adopting a forward-looking and strategic approach, the Council can continue to evolve its data protection framework in line with emerging legislation, technological advances, and public expectations.

3. Measures of success

3.1 Success will be demonstrated through:

- Sustained SAR compliance at or above 90% across all Services;
- Reduction in overdue SARs and escalation cases;
- Continued year-on-year reduction in personal data breaches;
- 100% compliance with mandatory training requirements;
- Consistent and timely completion of DPIAs for high-risk processing;
- Robust management and auditability of Schedule 2 requests and data sharing;
- Positive regulatory outcomes and reduced ICO complaints;
- Clear and regular assurance reporting to senior management and elected members; and
- Embedded information governance considerations within all major projects and digital initiatives.

4. Supporting documentation

None.



Rachel Blair
Chief Officer (Legal and Democratic)

5. Impacts

<p>5.1 Public Sector Equality Duty and Fairer Scotland Duty Does the report contain information that has an impact as a result of the Public Sector Equality Duty and/or Fairer Scotland Duty? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, please provide a brief summary of the impact?</p> <p>If Yes, has an assessment been carried out and published on the council's website? https://www.northlanarkshire.gov.uk/your-community/equalities/equality-and-fairer-scotland-duty-impact-assessments Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
<p>5.2 Financial impact Does the report contain any financial impacts? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, have all relevant financial impacts been discussed and agreed with Finance? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p>
<p>5.3 HR policy impact Does the report contain any HR policy or procedure impacts? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, have all relevant HR impacts been discussed and agreed with People Resources? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p>
<p>5.4 Legal impact Does the report contain any legal impacts (such as general legal matters, statutory considerations (including employment law considerations), or new legislation)? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, have all relevant legal impacts been discussed and agreed with Legal and Democratic? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact?</p> <p>The report contains legal impacts arising from the Council's statutory duties under data protection and information governance legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. These duties require the Council to maintain effective governance arrangements, comply with statutory timescales (particularly in relation to Subject Access Requests and breach reporting), and demonstrate accountability through appropriate policies, procedures, and assurance mechanisms.</p> <p>The report also reflects the Council's obligations to respond to regulatory oversight by the Information Commissioner's Office (ICO), including engagement where compliance performance falls below expected thresholds. Employment law considerations arise in relation to training requirements, role responsibilities, and the management of additional workload associated with SAR handling and information governance activity, all of which are managed within existing legal and HR frameworks.</p>

In addition, the report acknowledges forthcoming legislative and regulatory change, including the Data Use and Access Act, which will require ongoing review of policies, processes, and governance arrangements to ensure continued compliance.

5.5 Data protection impact

Does the report / project / practice contain or involve the processing of personal data?

Yes No

If Yes, is the processing of this personal data likely to result in a high risk to the data subject?

Yes No

If Yes, has a Data Protection Impact Assessment (DPIA) been carried out and e-mailed to dataprotection@northlan.gov.uk

Yes No

5.6 Technology / Digital impact

Does the report contain information that has an impact on either technology, digital transformation, service redesign / business change processes, data management, or connectivity / broadband / Wi-Fi?

Yes No

If Yes, please provide a brief summary of the impact?

Where the impact identifies a requirement for significant technology change, has an assessment been carried out (or is scheduled to be carried out) by the Enterprise Architecture Governance Group (EAGG)?

Yes No

5.7 Environmental / Carbon impact

Does the report / project / practice contain information that has an impact on any environmental or carbon matters?

Yes No

If Yes, please provide a brief summary of the impact?

5.8 Communications impact

Does the report contain any information that has an impact on the council's communications activities?

Yes No

If Yes, please provide a brief summary of the impact?

5.9 Risk impact

Is there a risk impact?

Yes No

If Yes, please provide a brief summary of the key risks and potential impacts, highlighting where the risk(s) are assessed and recorded (e.g. Corporate or Service or Project Risk Registers), and how they are managed?

The report identifies a number of key risks associated with information governance and data protection compliance.

The principal risks relate to non-compliance with statutory requirements under the UK GDPR and Data Protection Act 2018, particularly in relation to timely breach reporting and Subject Access Request (SAR) performance. Failure to meet statutory timescales or regulatory expectations could result in increased regulatory intervention by the Information Commissioner's Office (ICO), including enforcement action, reputational damage, loss of public trust, and potential financial penalties.

There is also an operational and organisational risk arising from increased demand for SARs and information rights activity, particularly in high-volume services such as Social Work. Without effective controls, this could impact service delivery, place pressure on staff resources, and increase the likelihood of errors or further breaches.

These risks are assessed and managed through the Council's established governance and risk management framework. Information governance risks are recorded and monitored through relevant Service Risk Registers, with escalation to the Corporate Risk Register where appropriate. Oversight is provided through the Data Governance Board, Business Management Team, and Corporate Management Team, supported by regular performance reporting on breaches, SAR compliance, and training uptake.

Mitigating actions include strengthened breach reporting and incident response processes, enhanced monitoring and reporting of SAR performance, clear ownership and accountability arrangements, targeted training and staff support in higher-risk service areas, and ongoing review of policies and procedures. Collectively, these measures provide assurance that risks are actively managed and kept under continuous review.

5.10 Armed Forces Covenant Duty

Does the report require to take due regard of the Armed Forces Covenant Duty (i.e. does it relate to healthcare, housing, or education services for in-Service or ex-Service personnel, or their families, or widow(er)s)?

Yes No

If Yes, please provide a brief summary of the provision which has been made to ensure there has been appropriate consideration of the particular needs of the Armed Forces community to make sure that they do not face disadvantage compared to other citizens in the provision of public services.

5.11 Children's rights and wellbeing impact

Does the report contain any information regarding any council activity, service delivery, policy, or plan that has an impact on children and young people up to the age of 18, or on a specific group of these?

Yes No

If Yes, please provide a brief summary of the impact and the provision that has been made to ensure there has been appropriate consideration of the relevant Articles from the United Nations Convention on the Rights of the Child (UNCRC).

If Yes, has a Children's Rights and Wellbeing Impact Assessment (CRWIA) been carried out?

Yes No