Bolsover, Chesterfield and North East Derbyshire District Councils'

Internal Audit Consortium

Internal Audit Report

Authority:	**Bolsover District Council**
Subject:	**Data Protection**
Date of Issue:	**14th October 2025**
Assurance Level	**Limited Assurance**
Report Distribution:	**Director of Governance and Monitoring Officer Information & Engagement Manager & Data Protection Officer Chief Executive Director of Finance & 151 Officer**

Introduction

In accordance with the 2025/26 Annual Audit Plan, a review of the processes and controls in respect of Data Protection has been undertaken.

The audit assessed the Council's arrangements against requirements of the Data Protection Act 2018 and UK data protection legislation, with focus on key areas of governance, transparency, training, records management, and breach handling. The audit was scoped and planned in consultation with the Council's Data Protection Officer (DPO).

Internal audit work and reporting has been carried out in line with the requirements of the Institute of Internal Auditors (IIA) Global Internal Audit Standards.

Executive Summary

The audit confirmed that the Council had made measurable progress in strengthening its data protection framework. A new Data Protection Policy (July 2025) has been developed to replace outdated documentation, public-facing webpages have been refreshed, and breach management arrangements were generally sound. Serious cases were appropriately escalated and reported to the ICO within statutory timescales.

Training content was relevant and targeted. However, the centralised training log was incomplete, limiting assurance over full workforce coverage. Records of Processing Activities (RoPA) had not been maintained and the Corporate Retention Schedule remained outdated and inaccessible on the intranet. Some internal guidance continued to reference legacy legislation and parental consent processes within Leisure Services were inconsistent across activities.

One historic data breach (from 2023) led to civil proceedings and a financial settlement, prompting the introduction of new internal policies on redaction to strengthen future controls.

The audit covered the period April 2024 to September 2025, capturing both legacy issues and subsequent improvements. Overall, while progress has been made under the new management structure, several areas still require attention to provide full assurance.

Background

Responsibility for data protection transferred to the newly established Information & Engagement Team in April 2025, following the permanent move of the previous DPO and Deputy DPO to North East Derbyshire District Council.

Since taking over, the team has initiated a structured compliance improvement programme aimed at embedding accountability and addressing weaknesses identified.

Key early actions have included the rollout of online Data Protection training to all employees, ensuring accessible delivery across both office-based and operational staff and the inclusion of the RoPA and Corporate Retention Schedule refresh within the Data Protection

Compliance and Work Programme 2024-25. These actions demonstrate that the Council is actively addressing deficiencies while building a more sustainable compliance framework for the future.

Assurance Opinion	
Limited Assurance	Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed.

For a full list of Assurance definitions linked to risk see Appendix 1. For definitions of High, Medium and Low risk recommendations see Appendix 2. For definitions of Root Cause Analysis see Appendix 3. For the Management Action Plan see Appendix 4.

Key Findings

- Progress has been made against all recommendations from the 2022/23 audit, with improvements noted in some areas. However, several actions - particularly those relating to policy approval, training records, privacy notices, the asset register and the retention schedule - remain partially implemented and have been re-tested in this review.
- A new draft Data Protection Policy has been prepared (July 2025) and represents a significant improvement but this has not yet been finalised or approved; staff-facing intranet pages remain outdated.
- The DPO and Deputy are visible across the organisation and qualified to advise on data protection matters.
- Training had been delivered, but centralised records showed only 305 of 513 filled posts with evidence of completion; refresher cycles were not recorded.
- Confidential waste disposal was secure. A contract and monitoring processes were also in place.
- The register of processing activity (asset register) had not been kept up to date and is a key document in terms of identifying data held by the Council and how it is used.
- Privacy notices were present on most forms but inconsistent in version control; supporting guidance (e.g. Data Disposal) was outdated.
- Parental consent processes were in place within Leisure Services, but practices were inconsistent across activities and some forms had not been updated in several years.
- The retention schedule dated 2018 remained in place and inaccessible on the intranet; service-level testing was therefore not repeated.
- Breach management was effective for high-risk cases, but the register contained incomplete closure information and occasional gaps in rationale.
- Committee report templates included DP implications, but duplicate and outdated guidance existed on ERIC.

- Job descriptions included standard data protection responsibilities.

Scope, Objectives and Risks

The objective of the audit was to assess the adequacy and effectiveness of the Council's arrangements for ensuring compliance with the **Data Protection Act 2018** and related UK data protection legislation.

The review examined the design and operation of key controls intended to safeguard personal data, promote accountability, and prevent unauthorised disclosure or misuse of information. Specific areas of focus included:

- Governance arrangements, including the role and visibility of the Data Protection Officer and Deputy.
- The adequacy and approval status of the Council's Data Protection Policy and supporting guidance.
- Staff awareness and training arrangements, including induction and refresher training and the maintenance of centralised records.
- The use and consistency of privacy notices and consent mechanisms, including parental consent for children's data.
- Retention and disposal of personal data, including the currency and accessibility of the corporate retention schedule.
- The identification, investigation, and reporting of data breaches.
- The inclusion of data protection considerations within committee reports and procurement contracts.
- Physical and electronic access controls to ensure data is stored securely and accessed appropriately.

The key risks considered were that:

- Personal data may be processed unlawfully or without a valid legal basis.
- Staff may lack sufficient awareness of data protection responsibilities.
- Policies, guidance, or records (e.g. training, retention schedules) may be outdated or incomplete.
- Inconsistent management of breaches, consent or retention could expose the Council to non-compliance with the Data Protection Act 2018 and reputational harm.

Effective Controls

The Council had formally appointed a qualified Data Protection Officer and Deputy, who had taken on a visible and proactive role across the organisation. They had attended directorate meetings and contributed to the Risk Management Group, helping to raise awareness of data protection responsibilities.

Committee report templates included a section on data protection implications, and our sample testing confirmed that these were being completed appropriately. HR job descriptions also consistently included a standard statement of data protection responsibilities, embedding accountability at the point of recruitment.

Awareness of breach reporting was high. Staff were escalating incidents appropriately, and serious cases were being notified to the ICO within statutory timescales.

Finally, arrangements for confidential waste disposal were secure in practice and electronic access controls over files were operating effectively, with no evidence of inappropriate access.

Findings and Recommendations

Data Protection Policy / Guidance

We reviewed the Council's published 2024 Data Protection Policy and found that it continued to reference the UK GDPR as the primary framework, with outdated hyperlinks to EU resources. Staff-facing intranet guidance also contained legacy references to the 1998 Act and the Data Protection Bill. This created a risk that staff may rely on inaccurate or inconsistent guidance, undermining compliance.

During the course of the audit, we were provided with a new draft Data Protection Policy (July 2025). This addressed many of the weaknesses identified, aligning with the DPA 2018, and setting out roles, responsibilities and links to related procedures. However, the policy had not yet been finalised or approved, and several sections contained placeholders. Until the draft is embedded, the Council remains reliant on outdated material.

See Recommendation R1

Data Protection Training

We reviewed central HR training records and reconciled them to the July 2025 establishment list. Training was being delivered corporately, with content aligned to the Data Protection Act 2018 and good practice, but the records were incomplete. Only 305 of 513 filled posts had evidence of attendance, meaning around 41% of staff could not be confirmed as trained. Analysis showed that many of these gaps related to operational or field-based staff, such as cleaners, drivers, refuse operatives, and tradespeople, who have limited computer access and are therefore harder to reach through standard e-learning. The log also did not record completion dates or refresher cycles.

This limited assurance over full organisational compliance creates a risk that training coverage is uneven, refresher sessions are missed, and operational staff may not receive proportionate awareness training, reducing staff understanding and increasing the likelihood of unintentional data breaches

Since the audit fieldwork concluded, the Information & Engagement Team has introduced a new online Data Protection training module available to all staff, including those in operational roles. This development represents a positive step towards improving coverage and consistency, although full assurance will depend on accurate recording and monitoring of completion rates in future cycles.

See Recommendation R2

Privacy Notices

We sampled a range of privacy notices and reviewed corporate guidance. Notices were generally present but varied in format and version control, and some contained outdated references to legislation. Corporate “Data Disposal Guidance” (2014) was also still in use.

Inconsistent and outdated notices create a risk that individuals are not fully informed of how their data will be used, weakening transparency obligations and potentially leading to complaints or regulatory challenge.

See Recommendations R3

Register of Processing Actities (RoPA)

We sought to confirm that the Council maintains a current and comprehensive Record of Processing Activities (RoPA), as required under the Data Protection Act 2018. This should take the form of a corporate data asset register, capturing details of personal data held, the purposes of processing, categories of recipients, retention periods, and the safeguards applied.

During the audit, no live data asset register was initially provided. However, through further enquiries, we obtained a version dating from the 2020/21 audit, structured with a tab for each service area and containing fields consistent with data mapping. While this demonstrates that a corporate register was developed previously, it has not been maintained or embedded into current practice. The register has not been updated since 2020/21, and the current Data Protection Officer was unaware of it being in active use.

Management confirmed that, following the appointment of a new Information & Engagement Officer, there are plans to refresh and embed an up-to-date live Data Asset Register as part of the Council’s ongoing compliance programme. This action is reflected (albeit in general terms) within the BDC Data Protection Compliance and Work Programme 2024–25.

In the absence of a current, owned, and regularly updated register, there is limited assurance that the Council has full oversight of its personal data processing activities. Data mapping underpins several other areas of compliance, including the accuracy of privacy notices, the application of retention schedules and the completion of Data Protection Impact Assessments (DPIAs).

See Recommendation R4

Consent

We found no standalone record of consent processes or evidence of how consent and withdrawal are documented within services. However, this issue is intrinsically linked to the absence of a current corporate Record of Processing Activities (RoPA), which should capture the lawful basis for processing, including consent where applicable. The related recommendation (R5) therefore addresses this area.

Parental Consent

We reviewed parental consent arrangements within Leisure Services and confirmed that processes were in place across a range of activities, including arts projects, Go! Play programmes, Extreme Wheels sessions, swimming lessons and outdoor activities. However, practices varied between services and some consent forms had not been updated for several years.

This inconsistency increases the risk that children's personal data may not always be processed in line with the requirements of the Data Protection Act 2018, potentially exposing the Council to compliance and reputational risks.

See Recommendation R5

Retention Schedules

We reviewed the Council's corporate retention and disposal schedule (2018). The framework set out appropriate retention periods and disposal actions, but had not been updated since 2019, was inaccessible on the intranet, and the intranet search function returned a 404 error.

Outdated and inaccessible retention guidance creates a risk that staff retain records longer than necessary or dispose of them prematurely, undermining the storage limitation principle under DPA 2018. It also prevented meaningful service-level testing of compliance.

See Recommendation R6

We further confirmed that review and update of the Corporate Retention Schedule was included within the 2024-25 Data Protection Compliance and Work Programme, which should ensure alignment with current legislation and improve accessibility for staff once completed.

Data Breaches

We reviewed the Council's breach register, supporting guidance and a sample of ten incidents recorded between January 2023 and August 2025. We found that staff were aware of the need to escalate breaches, high-risk cases were notified to the ICO within 72 hours, and corrective actions were implemented.

However, weaknesses in record-keeping were identified. Six of the ten cases appeared closed in practice but were still recorded as "open" and one case lacked documented rationale for the ICO and data subject notification decision. All breach entries in the sample recorded since April 2025 were accurate, current and fully supported by evidence. Incomplete registers reduce the Council's ability to evidence accountability and to learn lessons consistently.

During the course of the review, we noted that one historic data breach (from 2023) had resulted in civil proceedings and a financial settlement against the Council. The incident prompted a comprehensive review of breach management and redaction practices and led to the development of a new Compensation Policy for Data Protection Breaches and a Redaction Policy (both drafted October 2025). These documents aim to ensure fair and proportionate redress in any future cases, improve consistency in breach response and reduce the risk of similar incidents recurring. Although the case was exceptional, it illustrates the potential financial and reputational impact of data handling failures and reinforces the importance of consistent breach prevention and training.

Overall, the current breach management arrangements are operating effectively under the new team, with the identified weaknesses confined to historic records.

Recommendation: R7.

Committee Reports

We reviewed committee report templates, a sample of packs, and supporting guidance. Templates included a section on data protection implications, and sample reports demonstrated compliance. However, we noted duplicate and outdated versions of guidance on ERIC.

Duplication risks confusion over which documents staff should follow, undermining consistency of reporting. See Recommendation R8

Recommendations	
R1	**Data Protection Policy/ Guidance** **Recommendation**: The Council should ensure that its draft Data Protection Policy (July 2025) is finalised, approved, and published without delay. Before publication, placeholders and incomplete references should be updated and links to related policies and procedures completed. At the same time, outdated guidance should be reviewed and either updated or withdrawn, particularly: • Data Disposal Guidance (2014) – to be revised and aligned with the Data Protection Act 2018. • Intranet (ERIC) content - to be updated so that staff-facing guidance is consistent with current law and the updated corporate policy. Once approved, the new policy and supporting guidance should be communicated to staff and councillors, with older versions removed from circulation. **Risk: Medium**
Root Cause	**Standards & Policies**
R2	**Data Protection training** **Recommendation**: The Council should introduce a mandatory refresher cycle for all staff and record compliance against this requirement through maintenance of a comprehensive central training log. The log should: • Capture attendance at all data protection sessions (including bespoke or departmental events). • Record completion dates for each staff member. • Track refresher cycles and flag when refresher training is due. • Record outstanding training requirements, ensuring managers are able to monitor and escalate non-compliance within their teams. • Reconcile periodically against the establishment list to confirm coverage across the workforce. This will provide assurance that staff awareness is consistent across the organisation, support compliance with the Data Protection Act 2018, and reduce the risk of gaps in coverage or lapsed refresher training. **Risk: High**
Root Cause	**Competencies & Training**

R3	**Privacy notices template** **Recommendation**: The Council should develop and adopt a corporate privacy notice template and accompanying style guide and update its Privacy Notices Guidance to align with the Data Protection Act 2018 and current ICO expectations. Once approved, all services should review and update their existing privacy notices using the new template to ensure consistent content, formatting and version control. This will strengthen transparency, reduce inconsistency across departments, and ensure the Council meets its obligations under UK data protection legislation. **Risk: Medium**
Root Cause	**Standards & Policies**
R4	**Records of Processing Activity (Data Asset Register)** **Recommendation**: The Council should ensure that the planned work within the 2024–25 Data Protection Compliance and Work Programme to refresh and embed a live Data Asset Register is delivered as a priority. The register should capture, as a minimum: • The purposes of processing personal data. • Categories of data subjects and personal data processed. • Categories of recipients with whom data is shared. • Transfers of data outside the UK (if applicable). • Retention periods for personal data. • Security measures applied to protect the data. Ownership should be clearly assigned to the Data Protection Officer and the register should be reviewed and updated regularly. This will provide assurance that the Council has full oversight of its data processing activities and is meeting its statutory obligations under the Data Protection Act 2018. **Risk: High**
Root Cause	**Governance**

R5	**Children – Parental Consent** **Recommendation**: The Council should ensure that all services collecting children’s personal data adopt a consistent and up-to-date approach to parental consent. This should include: • Updating consent forms to ensure they align with the Data Protection Act 2018. • Standardising retention and disposal practices across services. • Providing corporate guidance and oversight from the DPO to ensure consistent practice and assurance across all Leisure activities. **Risk: Low**
Root Cause	**Governance**
R6	**Retention Schedules** **Recommendation**: The Council should complete the planned review and update of the Corporate Record Retention and Disposal Schedule, ensuring that it: • Aligns with current legislation, guidance, and operational practice. • Is published in an accessible location on the intranet. • Can be readily located by staff through a functioning search facility. Once updated, the DPO should seek assurance that service managers across directorates are applying the refreshed requirements consistently, supported by periodic checks of both paper and electronic records. Completing this action will ensure staff have access to an up-to-date and reliable framework for managing records, reducing the risk of over-retention or premature disposal, and will provide a sound basis for future assurance testing. **Risk: Medium**
Root Cause	**Governance**

R7	**Data Breaches** **Recommendation**: The Council should strengthen the administration of its breach log/register to ensure that each case record is complete and capable of demonstrating compliance with accountability requirements under the Data Protection Act 2018. In particular, the following should be treated as mandatory fields before a case is closed: • Date/time breach was discovered and date/time assessment completed (to evidence the 72-hour standard). • ICO notification decision, with rationale documented in all cases (whether “Yes” or “No”). • Data subject notification decision, with rationale documented in all cases. • Containment and corrective actions, with evidence of completion. • Closure date and confirmation of review by the DPO or Deputy. In addition, a regular quality assurance check (e.g. monthly) should be introduced to review all “open” cases to confirm whether they remain live or should be administratively closed. **Risk: Low**
Root Cause	**Process & Procedures**
R8	**Committee Reports** **Recommendation**: The Council should ensure that guidance and templates relating to exempt information are streamlined and maintained in a single, clearly signposted location on ERIC. This would reduce duplication and reinforce consistent application by report authors. **Risk: Low**
Root Cause	**Governance**

Appendix 1

Assurance Level	**Internal Audit Definition**	**Risk Register Link**
Substantial Assurance	There is a sound system of controls in place, designed to achieve the system objectives. Controls are being consistently applied and risks well managed.	Rare impact
Reasonable Assurance	The majority of controls are in place and operating effectively, although some control improvements are required. The system should achieve its objectives. Risks are generally well managed.	Possible / Unlikely impact
Limited Assurance	Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed.	Major impact
Inadequate Assurance	There are fundamental control weaknesses, leaving the system/service open to material errors or abuse and exposes the Council to significant risk. There is little assurance of achieving the desired objectives.	Critical Impact

Appendix 2

Indicative Definitions of High Medium and Low Recommendations

Risk	Definition
High	Risks that can have a catastrophic / severe impact on the operation of the Council or service - Must take action to mitigate or terminate if not possible to do so: - • Death, extensive injury, major permanent harm • Unable to function without government or other agency intervention • Significant impact on service objectives • Inability to fulfil obligations • Short to medium term impairment to service capability • Adverse national publicity, highly damaging, loss of public confidence • Major adverse local publicity • High risk of fraud being able to occur e.g., key internal controls are not operating or are missing • Direct link to a strategic risk occurring • A serious breach of legislation/ legal requirements leading to substantial financial penalties or severe breach of data protection (report to ICO) • Substantial loss or damage to Council assets/or information
Medium	Risks which have a noticeable impact on the service provided, will cause a degree of disruption to service provision / impinge on the budget - Check current controls and consider if others are required: - • Medical treatment required, semi-permanent harm up to 1 year • Short term disruption to service capability • Significant financial loss • Some adverse publicity, needs careful public relations • Isolated personal details compromised • Risk of fraud being able to occur • Direct link to identified operational risks occurring • A serious breach of organisational policies and procedures • A breach of legislation / legal requirements leading to a moderate financial impact • Loss or damage to Council assets, information • Previously agreed medium internal audit recommendations remain outstanding
Low	Risks where the impact and any associated losses will be minor • First Aid treatment, non- permanent harm up to 1 month, no obvious harm or injury • Minor / negligible impact on service objectives • Financial loss that can be accommodated at service level / minimal • Some public embarrassment, no damage to reputation, unlikely to cause any adverse publicity / internal only • Minimal risk of fraud • No direct link to operational or strategic risks • A minor breach of organisations policies and procedures • A minor breach of Legislation / legal requirements • Low risk of loss or damage to Council assets

Appendix 3

Root Cause Analysis Categories

Resources

Definition: the extent to which the service has sufficient, capable resources, enabling it to carry out all aspects of its operational duties efficiently and effectively.

Examples: functions that had been carried out by a now non-existent post have fallen through the gaps; services have only enough resources to carry out key aspects of operational delivery, meaning some lower priority tasks are not executed.

Competencies & Training

Definition: the extent to which staff are appropriately qualified, trained or experienced to carry out their role.

Examples: lack of training; inappropriate training; ineffective training plans; poor recruitment; poor training material

Systems

Definition: the extent to which systems are fit-for-purpose and support the service to carry out its operations effectively.

Examples: system processes are not available or are not effective, resulting in discrepancies or workarounds to get the required outcome, system processes are circumvented or duplicated manually. Processes are carried out manually where systems processes would be more efficient.

Motivation & Incentives

Definition: the extent to which factors such as organisational or personnel change have impacted on staff desire to carry out their role efficiently and effectively.

Examples: staff are feeling demotivated by a recent restructuring and removal of some posts, and do not feel that they should be taking on new responsibilities.

Standards & Policies

Definition: the extent to which expected standards have been made clear to staff and the necessary policies are in place to support these standards.

Examples: there is no policy/procedure in place; policies/procedures are out of date; policies/procedures have not been reviewed within appropriate timescales; policies etc. are difficult to locate/access; links in policies either do not work or are out of date.

Governance

Definition: the extent to which the service is governed by a clear structure that sets out the roles and responsibilities of officers, and the service is supported by appropriate risk management and control systems.

Examples: lack of assigned responsibility and accountability; failure to act / ignorance; intentional misleading by management to protect themselves; underqualified / trained Board members.

Process & Procedures

Definition: the extent to which established processes are operating effectively and are supported by defined procedures.

Examples: failure to follow set procedures (take care re materiality/proportionality); lack of separation of duties; controls being bypassed.

Accountability

Definition: the extent to which roles and responsibilities for decision-making have been defined and are accepted and acted on by all parties.

Examples: unclear expectations; avoiding responsibility; lack of management oversight; poor communication.

Assurance & Monitoring

Definition: the extent to which internal and/or external checking controls exist to monitor the effectiveness of, and provide assurance to, the service.

Examples: unclear responsibility; not identifying and/or taking action on recurring problems; checking the wrong things; under-sampling.

Human Error

Definition: relating to people and their actions, error caused by stress, fatigue, carelessness, communication breakdown.

Examples: Spreadsheet formulas are wrong, figures transposed / typed in wrong, data taken from or entered in the wrong fields.

Appendix 4

Management Action Plan

Report Title:	**Data Protection**	**Report Date: 14th October 2025**
		Response Due By Date: 4th November 2025

	Findings and Risk identified	**Recommendations**	**Risk (High, Medium, Low)**	**Agreed**	**To be Implemented By:**		**Comments**
					Officer	**Date**	
R1	**Data Protection Policy/ Guidance** The 2024 Data Protection Policy remained in place, referencing the EU GDPR and outdated intranet guidance. A draft July 2025 version had been prepared but not finalised; placeholders and incomplete references remained. **Risk:** Staff may continue to rely on inaccurate or inconsistent materials, reducing confidence in the Council's policy framework and undermining its ability to demonstrate compliance with accountability requirements.	The Council should ensure that its draft Data Protection Policy (July 2025) is finalised, approved, and published without delay. Before publication, placeholders and incomplete references should be updated and links to related policies and procedures completed. At the same time, outdated guidance should be reviewed and either updated or withdrawn, particularly: • Data Disposal Guidance (2014) – to be revised and aligned with the Data Protection Act 2018. • Intranet (ERIC) content - to be updated so that staff-facing guidance is consistent with current law and the updated corporate policy. Once approved, the new policy and supporting guidance should be communicated to staff and	**Medium**	Agreed with relevant Officers. Outdated guidance has been removed from Eric. Eric pages have been refreshed accordingly.	KB KB	Before end of Dec 2025. Complete	This policy is ready and will be presented to the next Customer Services Scrutiny meeting on Mon, 8th Dec 2025, after which, the document will be published.

	Findings and Risk identified	Recommendations	Risk (High, Medium, Low)	Agreed	To be Implemented By:		Comments
					Officer	Date	
		councillors, with older versions removed from circulation.					
R2	**Data Protection training** Data protection training was delivered corporately but records were incomplete. Only 305 of 513 filled posts had a training record (41% gap), with no refresher tracking or completion dates. Many unrecorded roles were operational (e.g. cleaners, drivers, refuse operatives, tradespeople) who have limited access to e-learning. **Risk:** Without accurate tracking of staff completion and refresher cycles, training coverage may be uneven, refresher sessions missed and the Council could face difficulty evidencing compliance with statutory training obligations under UK data protection legislation.	The Council should introduce a mandatory refresher cycle for all staff and record compliance against this requirement through maintenance of a comprehensive central training log. The log should: • Capture attendance at all data protection sessions (including bespoke or departmental events). • Record completion dates for each staff member. • Track refresher cycles and flag when refresher training is due. • Record outstanding training requirements, ensuring managers are able to monitor and escalate non-compliance within their teams. • Reconcile periodically against the establishment list to confirm coverage across the workforce.	**High**	Agreed with HR to rollout all data protection modules on SkillGate.	LC/KB	Sep 2025	All staff received refresh data protection training on 11/09/25 via SkillGate. Reminders were sent out on 25/09/25. HR have successfully captured an accurate log of all completion dates/records. KB has since delivered in person, bespoke GDPR training to the Housing department.
R3	**Privacy notices template**	The Council should develop and adopt a corporate privacy notice	**Medium**	Agreed with KB to have all	KB	Dec 2025	There is one last privacy notice to

	Findings and Risk identified	Recommendations	Risk (High, Medium, Low)	Agreed	To be Implemented By:		Comments
					Officer	Date	
	Privacy notices were present but inconsistent in content, format and version control. Some included outdated references to legislation. Corporate Privacy Notices Guidance was outdated, referencing 2014 practice and not aligned to DPA 2018. **Risk:** Without a refreshed template and programme of regular review, privacy notices risk becoming inconsistent, incomplete, or failing to meet statutory obligations. Staff may rely on incorrect guidance, resulting in inconsistent or non-compliant privacy notices.	template and accompanying style guide and update its Privacy Notices Guidance to align with the Data Protection Act 2018 and current ICO expectations. Once approved, all services should review and update their existing privacy notices using the new template to ensure consistent content, formatting, and version control. This will strengthen transparency, reduce inconsistency across departments, and ensure the Council meets its obligations under UK data protection legislation.	🟧	privacy notices updated by mid-December.			be updated before they are all reviewed by Kellie B and published in Dec 2025.
R4	**Records of Processing Activity (Data Asset Register)** The Records of Processing Activities (Data Asset Register) had not been maintained since 2020/21	The Council should ensure that the planned work within the 2024–25 Data Protection Compliance and Work Programme to refresh and embed a live Data Asset Register is delivered as a priority. The register should capture, as a minimum:	**High**	KB, KB and service managers currently working on populating the master document.	KB DPO	Jan 2026	Well underway. We have adopted the ICO's recommended ROPA template in the absence of recent activity. The

	Findings and Risk identified	Recommendations	Risk (High, Medium, Low)	Agreed	To be Implemented By:		Comments
					Officer	Date	
	and was not recognised by the current DPO. **Risk:** The absence of an up-to-date and embedded Records of Processing Activities represents a significant compliance gap under the DPA 2018	- The purposes of processing personal data. - Categories of data subjects and personal data processed. - Categories of recipients with whom data is shared. - Transfers of data outside the UK (if applicable). - Retention periods for personal data. - Security measures applied to protect the data. Ownership should be clearly assigned to the Data Protection Officer and the register should be reviewed and updated regularly. This will provide assurance that the Council has full oversight of its data processing activities and is meeting its statutory obligations under the Data Protection Act 2018.	🟥				document is currently in draft format. Once all service managers have responded, it will be up to date by end of Jan 2026.
R5	**Children – Parental Consent** Parental consent processes were in place across Leisure Services activities (e.g. arts projects, Go! Play, Extreme	The Council should ensure that all services collecting children's personal data adopt a consistent and up-to-date approach to parental consent. This should include:	**Low**	We have just finished creating a corporate consent form for all services to access.	KB	Nov 2025	KB is working with Comms to update all their filming and photography policies. KB has refreshed

	Findings and Risk identified	Recommendations	Risk (High, Medium, Low)	Agreed	To be Implemented By:		Comments
					Officer	Date	
	Wheels, swimming lessons, outdoor activities). However, practices varied between services and some consent forms had not been updated for several years, leading to inconsistent approaches. **Risk:** Inconsistent and outdated parental consent processes increase the risk that children's personal data may be processed unlawfully, exposing the Council to compliance and reputational risks.	• Updating consent forms to ensure they align with the Data Protection Act 2018. • Standardising retention and disposal practices across services. • Providing corporate guidance and oversight from the DPO to ensure consistent practice and assurance across all Leisure activities.	🟩				consent protocols across services requiring child consent.
R6	**Retention Schedules** The corporate retention schedule (2018) was outdated, not updated since 2019, inaccessible on the intranet, and not locatable via search. **Risk:** Staff may be unable to apply retention rules consistently, leading to over-retention or premature deletion of records. It also limited audit's ability to confirm compliance at service level.	The Council should complete the planned review and update of the Corporate Record Retention and Disposal Schedule, ensuring that it: • Aligns with current legislation, guidance, and operational practice. • Is published in an accessible location on the intranet. • Can be readily located by staff through a functioning search facility. Once updated, the DPO should seek assurance that service managers across directorates are applying the refreshed	**Medium**	The first draft of the updated schedule is currently in review with service managers.	KB & KB	Jan 2026	The refreshed Retention Schedule is aligned with current legislation and will be ready for publishing in January 2026.

	Findings and Risk identified	Recommendations	Risk (High, Medium, Low)	Agreed	To be Implemented By:		Comments
					Officer	Date	
		requirements consistently, supported by periodic checks of both paper and electronic records. Completing this action will ensure staff have access to an up-to-date and reliable framework for managing records, reducing the risk of over-retention or premature disposal, and will provide a sound basis for future assurance testing.	🟧				
R7	**Data Breaches** Breach management was effective for high-risk cases, but weaknesses in register administration were noted: six cases open when effectively closed, and one lacking rationale for ICO/data subject notification. **Risk:** Incomplete data breach records reduce the reliability of management information and weaken the Council's ability to demonstrate accountability under the DPA 2018.	The Council should strengthen the administration of its breach log/register to ensure that each case record is complete and capable of demonstrating compliance with accountability requirements under the Data Protection Act 2018. In particular, the following should be treated as mandatory fields before a case is closed: • Date/time breach was discovered and date/time assessment completed (to evidence the 72-hour standard). • ICO notification decision, with rationale documented in	**Low**	This item relates to the 2024-25 register which was administered by the previous team. Since taking over the department in April 2025, I have ensured that the 2025-26 register is 100% up to date.	KB & KB	Apr-present	No risk. Item is 100% accurate.

	Findings and Risk identified	Recommendations	Risk (High, Medium, Low)	Agreed	To be Implemented By:		Comments
					Officer	Date	
		all cases (whether “Yes” or “No”). - Data subject notification decision, with rationale documented in all cases. - Containment and corrective actions, with evidence of completion. - Closure date and confirmation of review by the DPO or Deputy. In addition, a regular quality assurance check (e.g. monthly) should be introduced to review all “open” cases to confirm whether they remain live or should be administratively closed.					
K	Committee Reports Committee report templates included DP implications, but duplicate and outdated versions of guidance existed on ERIC. Risk: Duplication of guidance on ERIC could reduce clarity and consistency in reporting.	The Council should ensure that guidance and templates relating to exempt information are streamlined and maintained in a single, clearly signposted location on ERIC. This would reduce duplication and reinforce consistent application by report authors.	Low	Please see R1. Out of date guidance has been removed from ERIC. There are still a few forms which need to be split from NEDDC. These will be updated ASAP.	KB is in the process of updating forms relating to data protection making them BDC-specific.	Jan 2026	KB is monitoring KB’s progress. Vast improvements have been made on the main data protection page on ERIC: See Data protection

Please tick the appropriate response (✓) and give comments for all recommendations not agreed.

Signed Head of Service:	K B	Date:	1st Dec 2025

Note: In respect of any High Risk recommendations please forward evidence of their implementation to the Internal Audit team as soon as possible.