

Audit and Governance Committee

24 September 2026



Reading
Borough Council
Working better with you

Title	Information Governance Update
Purpose of the report	To note the report for information
Report status	Public report
Executive Director/ Statutory Officer Commissioning Report	Louise Duffield, Executive Director of Resources
Report author	Nayana George, Information Rights Services Manager Anrul Ullah, Interim Director Digital & IT
Lead Councillor	Cllr Ruth McEwan, Lead Councillor for Corporate Services and Resources
Council priority	Not applicable, but still requires a decision
Recommendations	The Committee is asked to: 1. Note the progress to date and future actions outlined in this report 2. Identify matters of interest for future reports

1. Executive summary

- 1.1. This report provides an update on the ongoing work to monitor and continuously improve the Council's policies, systems and processes around Information Governance.

2. Policy context

- 2.1. The Council Plan has established five priorities for the years 2025/28. These priorities are:
 - Promote more equal communities in Reading
 - Secure Reading's economic and cultural success
 - Deliver a sustainable and healthy environment and reduce our carbon footprint
 - Safeguard and support the health and wellbeing of Reading's adults and children
 - Ensure Reading Borough Council is fit for the future
- 2.2. Full details of the Council Plan and the projects which will deliver these priorities are published on the Council's website - [Council plan - Reading Borough Council](#). These priorities and the Council Plan demonstrate how the Council meets its legal obligation to be efficient, effective and economical. Data is playing an increasing role in designing, delivering and transforming public

services to improve outcomes for customers and drive efficiencies within current financial constraints.

2.3. The Local Government Association describe the value of data to public services as facilitating:

- The design of services around user needs
- The engagement and empowerment of citizens to build their communities
- Efficiencies and public service transformation
- Economic and social growth
- Greater transparency and accountability

2.4. Effective information governance is a key requirement for the Council which has duties to be both open and transparent whilst at the same time protecting the confidential information it holds about people and businesses.

3. Subject Access Requests Q1 & Q2 (1st April 2026 to 7th August 2026)

3.1. Across the Council (excluding Children's Services) a total of 68 cases were received in this reporting period (Q1 & Q2 of 2026/27). In September 2025 we reported to this committee that 81 cases were received in Q1 and Q2 up to 15th September 2025.

3.2. Of the 68 cases, 12 were closed as invalid requests and 2 cases have been closed as service requests. Of the remaining received in this reporting period, 11 have been completed and 33 remain outstanding. 10 of the outstanding cases are on hold awaiting receipt of identification and/or consent from the customer.

3.3. We report on Children's Services requests separately to capture the data for the Annual Complaints Report and any Ofsted inspections. Ofsted are interested in data relating to children and young people. These are predominantly:

- request from parents of children open to services;
- directly from young people who are currently in care;
- or adults who were in care when they were children.

3.4. A total of 60 cases were received for Children's Services in this reporting period (Q1 & Q2 of 2026/27). In September 2025 we reported to this committee that 57 cases were received in Q1 and Q2 up to 15th September 2025.

3.5. 12 cases have been closed as invalid requests and 0 have been closed as service requests. Of the remaining 48 cases 4 have been completed and 31 remain outstanding. 10 of the outstanding cases are currently on hold waiting identification verification and/or consent to be provided and 4 further case are on hold awaiting further information/clarification of the request from the customer.

3.6. Subject Access Requests (SARs) require careful review to ensure that whilst disclosing information to the individual, the Council does not breach data protection requirements or release confidential information. Appropriate redaction is therefore a critical stage of the SARs process, and the Council has been working to utilise software to support staff to complete this efficiently and effectively.

3.7. We reported to the committee in April 2026 that Officers were developing the specification for the procurement of redaction software and undertaking soft market testing, including demonstrations from several new suppliers. This work

is being support jointly by the Information Governance Team, the Procurement Team and the Digital & IT Service.

- 3.8. We have identified a preferred supplier through a framework and progressing the procurement exercise with a view to making a direct award by October 2026.
- 3.9. Over the last 3 years there has been a significant increase in the volume of SARs received. At the same time, the use of AI to draft requests for SARS have added to the complexity of these cases. Data subjects are more aware of their rights to access their information and using AI generated emails they challenge the responses sent. These factors have led to a backlog in SARs processing. The table below provides a summary of the position as of 30th June 2026.

	2020/21		2021/22		2022/23		2023/24		2024/25		2025/26		2026/27	
	RBC	BfC	RBC	BfC	RBC	BfC	RBC	BfC	RBC	BfC	RBC	DoCS	RBC	DoCS
No. received	35	64	44	38	46	59	80	75	145	58	203	128	18	19
No. outstanding	0	0	0	0	0	0	1	1	4	6	18	33	8	6
No. on hold (Requires further info)	0	0	0	0	0	1	0	0	0	0	1	0	0	1
No. on hold (No consent / ID)	0	0	0	0	0	0	0	0	0	0	1	0	2	5
No. Completed	35	64	44	38	45	54	68	62	50	24	40	36	3	3
No. Declined (Invalid request ¹)	0	0	0	0	1	4	11	12	89	28	116	56	5	4
No. Declined (Service request)	0	0	0	0	0	0	0	0	1	0	27	3	0	0

4. Freedom of Information (FOI) requests

- 4.1. In accordance with the Information Commissioners Office (ICO) guidelines, we are monitoring and reporting the number of cases responded to vs number of cases responded to in timescale.
- 4.2. The table below shows the total number of FOI's received in Q1 of 2026/27, split by each Directorate.

¹¹ Invalid request: requests that have been submitted without ID or Proof of Address, no response to requests to provide, 6 week time limit passed (as per ICO Guidelines)

Directorate	Total Number Received Q1 26/27
Children's Services & Education	53
Communities, Adult Social Care & Housing	43
Environment, Growth & Neighbourhood Services	218
Resources	91
Total	405

- 4.3. The table below shows the total number of FOI's responded to within timescales in Q1 of 2026/27 which is 77.6%.

Directorate	Total Number responded to in timescale Q1 26/27
Children's Services & Education	29
Communities, Adult Social Care & Housing	26
Environment, Growth & Neighbourhood Services	176
Resources	71
Total	302 (77.6%)

- 4.4. In September 2025 we reported that a total of 312 FOI requests were received in Q1 and 310 of these were responded to in timescales whereas in 2026/27 Q1 the Council received a total of 405 requests and 302 of these were responded to in timescales which is 77.6%. Whilst response rates have dropped, we must recognise that a total of 93 extra requests or 29% were received. We are also seeing that requests generated using AI are being received regularly which are complex and lengthy, often with multiple questions per request. And these require responses from multiple teams across the organisation. System generated email reminders are being sent to Responders at key intervals to encourage timely responses. Reports outlining Overdue and Upcoming requested are provided to Executive Directors and Directors to provide an overview within service areas on a weekly basis. Executive Directors and Directors also have direct access to the system to monitor more frequently and access any detailed information required to support a response.
- 4.5. During this reporting period there were 10 requests for Internal Review of Freedom of Information responses. 6 were completed with the Council's original response upheld and 2 were completed with additional/amended information and 2 are open still at review stage.

Improvement Actions

- 4.6. Following the commissioning of the Change Delivery Team to undertake a comprehensive review of the following processes: Complaints, Freedom of Information (FOI) Requests, and Subject Access Requests (SAR) we have an action plan for the service to work with colleagues in Customer Services to strengthen how the organisation responds to issues raised on behalf of residents, ensure resources are deployed effectively, and promote a more efficient and consistent approach across all enquiry types.
- 4.7. Where customers use the webform to make their request it significantly reduces the processing time as the information is fed directly into the system, rather than being copied into the system by Officers. As well as providing more capacity for Officers to work with Responders to complete timely responses, this also reduces the risk of errors. We will, therefore, continue to promote the webform as the most effective way to submit requests. Further we will be reviewing the webform so as to make sure we understand clearly and concisely the matters being raised.
- 4.8. Case allocation emails are automatically generated by the case management system to support responders to monitor requests and meet deadlines. Feedback has identified that these are not always easy to manage, particular for services with higher case volumes. Whilst improvements have therefore been made to make these easier to view and read for Responders and Approving Managers, further improvements to the system are being considered following feedback from the organisation.
- 4.9. A key method of reducing repeat demand within FOIs is to ensure that information is easily accessible for customers. Where information is already published and easy to find it removes the need for customers to submit an FOI. Officers have established an FOI Publication Log to support this work, which ensured customers to self-serve and review the log before submitting a new FOI request.
- 4.10. Council wide training is being planned from October 2026 onwards to improve consistency and raise standards by improving understanding of the process, requirements and responsibilities.

5. Data Transparency

- 5.1. The Data Transparency web pages are up to date for Contracts costing over £5,000 with data for Q1 and Q2 2026 is published.
- 5.2. Expenditure over £500 for Q1 as of 2026/27 is published.
- 5.3. The Pay Policy Statement and Trade Union faciality time will be updated once this information has been prepared and been approved via Personnel Committee.

6. Information Governance Board

- 6.1. The Information Governance Board meets monthly and reviews Cyber Security Incidents and possible breaches of the Data Protection Act which may need to be reported to the Information Commissioners Office (ICO).
- 6.2. As part of good information governance, it is essential that the Council has a culture where staff are encouraged to report any data related incidents swiftly.

This is supported and reinforced by mandatory annual training, which is updated each year to incorporate learning and themes from the previous year.

- 6.3. There were 49 data related incidents reported to the Information Governance Team in Q1. This was around average as for the previous two Q3 and Q4 where there was a combined total of 105 reports logged with IG Team. Q1 and Q2 of 2025/26 94 incidents were reported.
- 6.4. None of breaches met the criteria for notifying the ICO.
- 6.5. The main theme from data breaches has been identified as misdirection of emails and postal communications as a result of human error, rather than any systemic or governance failures.
- 6.6. All breaches are discussed at the Information Governance Board and where subsequent actions are identified these are monitored by the Board. Actions have included specific training and improvement action plans for services.
- 6.7. Regular internal communications messaging is used to encourage checking that the correct recipients and their addresses (email and postal) are correct before sending. The ICO's Preventative Measures Leaflets are sent out following a breach. A copy of any ICO Decision Notices, along with their recommendations, are provided to relevant Service Managers and staff.

7. Information Management Strategy

- 7.1. The Information Management Strategy and Action Plan was presented and signed off by the Policy Committee in March 2022. This sets out the Council's approach to information management and governance.
- 7.2. The Action Plan from this has since been adapted to align to the ICO's template. This allows for better tracking and reporting of actions completed.
- 7.3. The Action Plan is supported by a team of Data Stewards operating at both service at corporate levels across the organisation. They are also responsible for promoting good data management.
- 7.4. The Information Governance Team has successfully recruited two new members of staff. This will allow capacity to support the Data Stewards.
- 7.5. The Information Governance Team Data Stewards site on SharePoint and the Intranet provides access to guidance, templates and processes that Data Stewards require to complete work outlined in the Action Plan and to support their teams and colleagues.
- 7.6. Further work to update the external website to share information and ensure transparency about how the Council work to the Data Protection Act will be completed as capacity in the team has now increased.
- 7.7. The Data Use and Access Act 2025 (DUAA)

The DUAA is a new Act of Parliament that updates some laws about digital information matters. One significant change that affected Reading Borough Council is that we now have a process in place for processing Complaints specifically around Data Protection, this was from 19th June 2026.
- 7.8. The Complaints process is published on the Council's website, and we are currently responding to a number of complaints about data protection matters. A summary of these will be made available to this committee at the April 2027 meeting.

8. Training

- 8.1. Cyber Security and Information Governance (GDPR) training is a mandatory requirement within the Council.
- 8.2. The training is available to all staff and councillors through Learning Pool, the Council's e-learning package.
- 8.3. Completion rates of these two training courses are monitored regularly by senior managers and HR and Organisational Development Service. This enables managers to take appropriate action to encourage their staff to complete the training. Ultimately, where training is not completed access to system can be reduced or removed to protect the Council.
- 8.4. The figures will be available at the April 2027 committee meeting as the next round of refresher training is currently being undertaken and we expect this to be completed by the end of October 2026.
- 8.5. The Information Governance Team will continue to provide bespoke advice, training and support for colleagues. This includes for those without access to IT systems.

9. Cyber Security Programme

- 9.1. The Audit & Governance Committee requested an update regarding the cyber security programme, in recognition of the seriousness with which this matter is considered within the Strategic Risk Register.
- 9.2. It is important to recognise that cyber security is a significant risk for all organisations, and not just the Council. The high-risk rating should not, therefore, be seen as an indication that the Council is failing to take the necessary actions to protect itself.
- 9.3. The following section provides an update on some of the risks that we are facing and the actions being taken.

Cyber incidents

- 9.4. The Council has seen an increase in malicious emails originating from legitimate supplier accounts that have been compromised by threat actors. This reinforces the importance of supply chain security and the Council's approach to third-party assurance, whereby suppliers are required to evidence compliance with recognised cyber security standards and good practice as part of procurement and contract management processes.
- 9.5. The Council's cyber security controls continue to prevent the vast majority of malicious activity from reaching users. 80% of all inbound email traffic was identified as unwanted or malicious and automatically blocked by the Council's security systems before delivery.
- 9.6. During the reporting period, additional measures have been introduced to strengthen the Council's cyber resilience. These include a password assurance exercise to identify weak credentials, enhanced controls restricting access from overseas locations, and ongoing development of a Secure Access Service Edge (SASE) solution to further protect Council services and data.
- 9.7. These controls have already demonstrated their effectiveness. With two attempted account compromise incidents were successfully contained after users responded to phishing emails. The attackers were prevented from

accessing Council systems due to existing security controls, and the affected accounts were immediately secured.

- 9.8. The cyber threat to local government remains significant, with councils continuing to be targeted by phishing, credential theft, ransomware and other malicious activity. The Council will therefore continue to invest in cyber security controls, staff awareness, independent security testing, and continuous monitoring to maintain an appropriate level of protection.
- 9.9. At the meeting in April 2026, the Committee received data regarding incoming emails that had been blocked as part of the Council's cyber security. There was a peak in February 2025, and further details were requested.
- 9.10. The volume of spam and suspicious emails received by the organisation is inherently variable and influenced by a range of external factors, including changes in attacker activity, the emergence of new phishing campaigns, global cybersecurity events, and the effectiveness of upstream email filtering services. As a result, email threat volumes can fluctuate significantly over time and should not be expected to follow a consistent pattern.

Month	Quantity of inbound emails automatically blocked	% of all inbound emails
May 2025	4,405,655	86.00%
June 2025	3,688,091	83.20%
July 2025	3,605,594	82.70%
August 2025	3,610,978	84.50%
September 2025	3,562,605	82.10%
October 2025	3,511,244	81.40%
November 2025	3,572,952	82.80%
December 2025	3,396,004	83.30%
January 2026	3,464,976	82.00%
February 2026	3,173,249	81.50%
March 2026	3,670,857	81.80%
April 2026	3,472,057	82.30%
May 2026	3,399,931	82.40%
June 2026	3,800,443	82.10%

Security Updates

- 9.11. The Service has recently conducted a password cracking exercise on all staff to uncover any weak passwords. Staff whose passwords have been compromised during this exercise have been contacted and forced to change their password to adhere to our security standards.
- 9.12. Will be commissioning an external Penetration Test in the next month for security assurance.

10. Contribution to strategic aims

- 10.1. The purpose of Information Governance is cross-cutting and relevant to all Services of the Council and to all of our public facing services which collect and retain data about the public.

11. Environmental and climate implications

- 11.1. There are no implications in relation to this report.

12. Equality Implications

- 12.1. All citizens have rights to information. There is no evidence that any section of the community is disadvantaged in accessing those rights under the current service provision.

13. Legal implications

- 13.1. How the Council collects, uses, stores, shares and destroys personal data is governed by the Data Protection Act.
- 13.2. The Council also has to comply with the Freedom of Information Act, the Environmental Information Regulations and the Access to Information Act in relation to its records. Compliance is monitored by the Information Commissioner who has wide ranging powers including the ability to impose considerable financial penalties for breaches of the Data Protection Act.
- 13.3. Effective governance, policies and practices are essential to minimising the risk of data protection breaches and to help ensure the appropriate handling of information requests. Failure to do so could result in regulatory action being taken against the Council.

14. Financial implications

- 14.1. There are no direct financial implications arising from this report.

15. Background papers

- 15.1. There are none.