Audit and Governance Committee

08 April 2026

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 Ade Marques, Director Digital & IT
Lead Councillor	Cllr Ellie Emberson, 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 actions in progress to 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 Q3 & Q4 (1st October 2025 to 16th March 2026)

3.1. Across the Council (excluding Children's Services) a total of 92 cases were received in this reporting period, compared to the 81 cases received in Q1 & Q2.

3.2. 56 cases were closed as invalid requests. Of the remaining 36 cases received in this reporting period, 12 have been completed and 24 remain outstanding. 1 of the outstanding cases is on hold awaiting receipt of identification and/or consent from the customer.

3.3. We report on Children's Services requests separately. 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 58 cases were received for Children's Services, compared to the 57 received in Q1 and Q2. 19 cases have been closed as invalid requests. Of the remaining 39 cases, 4 have been completed and 25 remain outstanding. 1 of the outstanding cases is currently on hold waiting identification verification and/or consent to be provided.

3.5. 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.

3.6. Unfortunately, the current redaction software is not meeting our requirements following rigorous testing and as a result staff are reliant on more manual processes whilst a new procurement exercise is undertaken. Officers are currently developing the specification for this procurement 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.

3.7. Over the last 3 years there has been a significant increase in the volume of SARs received. At the same time, the complexity of these cases has also increased. These two factors have led to a backlog in SARs processing. The table below provides a summary of the position as of 16 March 2026.

	2020/21		**2021/22**		**2022/23**		**2023/24**		**2024/25**		**2025/26**	
	RBC	BFfC	RBC	BFfC	RBC	BFfC	RBC	BFfC	RBC	BFfC	RBC	DoCS
No. received	**35**	**64**	**44**	**38**	**46**	**59**	**80**	**75**	**144**	**58**	**190**	**122**
No. outstanding	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**9**	**11**	**35**	**50**
No. on hold (Requires further info)	0	0	0	0	0	0	0	0	0	0	0	1
No. on hold (No consent / ID)	0	0	0	0	0	0	0	0	0	0	2	11
No. Completed	**35**	**64**	**44**	**38**	**45**	**54**	**68**	**62**	**49**	**23**	**30**	**25**
No. Declined (Invalid request[1])	0	0	0	0	1	4	11	12	86	24	99	35
No. Declined (Services request)	0	0	0	0	0	0	0	0	0	0	24	0

4. Freedom of Information (FOI) requests

4.1. As previously reported, a number of measures have been taken with the aim of increasing FOI performance:

- Centralisation of the function in the Customer Relations Team
- Implementation of a new case management system
- Review of the procedures
- Training has been provided to Officers
- Continual monitoring weekly by CMT

4.2. 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.

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

4.3. The table below shows the total number of FOI’s received in Q1 and Q2 of 2025/26.

Directorate	**Total Number Received Q1**	**Total Number Received Q2**
Children’s Services & Education	40	52
Communities, Adult Social Care & Housing	58	59
Environment, Growth & Neighbourhood Services	115	167
Resources	99	84
Total	**312**	**362**

4.4. The table below shows the total number of FOI’s responded to within timescales in Q1 and Q2 of 2025/26.

Directorate	**Total Number responded to in timescale Q1**	**Total Number responded to in timescale Q2**
Children’s Services & Education	44	36
Communities, Adult Social Care & Housing	59	52
Environment, Growth & Neighbourhood Services	110	164
Resources	97	75
Total	**310 (87%)**	**327 (87%)**

4.5. The following table shows the number of FOI cases received in Q3 and up to 23 March of Q4 of 2025/26.

Directorate	**Total No Received Q3**	**Total No Received Q4**
Children’s Services & Education	57	46
Communities, Adult Social Care & Housing	44	43
Environment, Growth & Neighbourhood Services	141	165
Resources	81	80
Total	**323**	**334**

4.6. Tables below show the total number of FOI's responded to in Q1 of 2025/26 by Directorate was 73% and in Q4 to date it is at 77.6%.

Directorate	Total Number responded to in timescale Q3	Total Number responded to in timescale Q4
Children's Services & Education	64	38
Communities, Adult Social Care & Housing	47	43
Environment, Growth & Neighbourhood Services	148	151
Resources	87	78
Total	**346 (73%)**	**310 (77.6%)**

4.7. Q1 and Q2 saw improvements in the timescales for responses, with a slight reduction in Q3. There was improvement in Q4, although still below the performance in the first half of the year. 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 Director and Directors to provide an overview within service areas. Executive Director and Directors also have direct access to the system to monitor more frequently and access any detailed information required to support a response.

4.8. During this reporting period there were 18 requests for Internal Review of Freedom of Information responses. 11 were completed with the Council's original response upheld and 7 are open still at review stage.

Improvement Actions

4.9. We recognise that improvements need to be consistent and the Change Delivery Team has been commissioned to undertake a comprehensive review of the following processes: Complaints, Freedom of Information (FOI) Requests, and Subject Access Requests (SAR).

4.10. The purpose of this review is 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.

4.11. Where customers use the webform to making 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.

4.12. 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. Improvements have therefore been made to make these easier to view and read for Responders and Approving Managers.

4.13. 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 are establishing an FOI Publication Log to support this work, which will allow customers to self-serve and review the log before submitting a new FOI request.

4.14. Council wide training will be carried out 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 Q1-3 of 2025/26 published.

5.2. Expenditure over £500 for Q1-3 and first 2 months of Q4 of 2025/6 is also published. Information related to April is currently being drafted ready for publication.

5.3. The Constitution was updated in October 2025 to reflect the changes to the Directorate of Children's Services coming back into the Council. The senior management structure chart is also up to date. Areas where annual changes are required will be completed by the end of April, such as the Fraud data and Pay policy statement.

5.4. At the last Committee we reported that the Parking Services accounts and Parking Annual Report for 2025/25 required publishing. This is now complete.

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 105 data related incidents reported to the Information Governance Team in Q3 and Q4 to date. This is an increase from Q1 & Q2 when 94 incidents were reported.

6.4. One report from Q3 met the criteria for notifying the ICO. This incident involved the disclosure, via email, of court documents issued to a parent. The disclosure was fully investigated and the cause was identified as incorrect instructions about sharing information for this case within the social care case management system. Swift action has been taken to update with the correct information. The data was confirmed as deleted by the parent's solicitor. The ICO recommended no further action for the Council on this matter.

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. Due to the impact of staff absences and turnover within the specialist Information Governance Team, there has been limited support provided to the Data Stewards over the last year. The Council is in the process of recruiting into roles within the team, including apprenticeship positions. This will provide additional capacity and enable the work with the Data Stewards to continue.

7.5. Despite the above issue, the Information Governance Team has created and maintained a Data Stewards site on SharePoint. This 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 once current recruitment has been successfully completed.

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 the Mandatory Training Task & Finish Group. 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. As a result, the Council has a high completion rate for these courses:

• Cyber Security	90.28%
• GDPR	91.50%

8.5. These figures include staff who do not use IT equipment.

8.6. The figures will be impacted by some staff that may be on long term sick leave, maternity leave or any new starters who are waiting to complete the training.

8.7. Over 600 members of staff provided positive feedback on the new format of the training and have made suggestions to improve it further by including more audio and video content. With the feedback and advice received from the ICO and learning from the breach management process, the Cyber Security and GDPR training is being revised in readiness for the 2026/27 roll out.

8.8. 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. Next Steps

9.1. In the next period, the of the Information Governance Team will be:

- Identifying and implementing improvements to processes resulting from the review project
- Successful recruitment into vacant roles
- Further improvements to the Cyber Security and GDPR training content, for the coming year
- Procurement of new redaction software to support safe, effective and efficient SARs processing.
- Recommencing work with the Data Stewards Network.

10. Cyber Security Programme

10.1. 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.

10.2. 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.

10.3. The following section provides an update on some of the risks that we are facing and the actions being taken.

Cyber incidents

10.4. We continue to see more sophistication in the cyber threats facing the Council, with email a particular channel for these attacks. Common attacks include

- Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person
- Malware is software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
- Drive by download attack refers to the unintentional download or malicious code to a computer or mobile device that leaves it open to a cyberattack.

10.5. The scale of these attempts is significant. Between January and March 2025 the Council recorded over 20,000 attempted phishing attacks each month. The volume of malware and drive by attempted attacks has been consistently over 1,000 each month, but has peaked at over 25,000 attacks in December 2025.

10.6. The Council has a number of tools designed to identify and automatically remove these before they reach users. Phishing attacks have dramatically declined as a result.

10.7. The table below provides a summary of the incoming mail blocked by our cyber security tools.

Month	Quantity of inbound emails automatically blocked	% of all inbound emails
January 2025	3,212,538	80.70%
February 2025	11,616,034	94.40%
March 2025	7,595,422	90.80%
April 2025	4,441,740	86.30%
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%

Security Updates

10.8. The Council has recently implemented Microsoft defender P2 to provide ongoing automated investigation remediation, threat hunting and treat analytics to our Microsoft 365 estate.

10.9. This is currently the highest tier or protection Microsoft offers which we have implemented for majority of the council’s estate.

10.10. Further rollout of Defender P2 is planned for field workers in the coming months.

10.11. The council is currently in conversations partners to redesign the IT network infrastructure to move it closer to a zero-trust cloud-based network connective model to improve security and performance.

10.12. A security review on the use and security of Council devices and network is planned.

11. Contribution to strategic aims

11.1. 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. The role of Information Governance contributes to the Corporate Priority foundation of “Getting the best value”.

12. Environmental and climate implications

12.1. There are no implications in relation to this report.

13. Community engagement

13.1. No consultation is planned in relation to the Information Management Strategy or Action Plan. It will, however, be in the public domain via published reports and updates.

14. Equality Implications

14.1. 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.

15. Legal implications

15.1. How the Council collects, uses, stores, shares and destroys personal data is governed by the Data Protection Act.

15.2. 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.

15.3. 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.

16. Financial implications

16.1. There are no direct financial implications arising from this report.

17. Background papers

17.1. There are none.