Audit and Governance Committee

25 September 2025

Title	Information Governance Quarterly 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	Michael Graham, Assistant Director of Legal and Democratic Services Ade Marques, Assistant 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. To note the progress to date and future actions outlined in this report 2. To 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. In delivering these priorities, we will be guided by the following set of principles:

- Putting residents first
- Building on strong foundations
- Recognising, respecting, and nurturing all our diverse communities
- Involving, collaborating, and empowering residents
- Being proudly ambitious for Reading

2.3. 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.

2.4. 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.

2.5. 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

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

3. Update

Subject Access Requests Q1 & Q2 (1st April 2025 to 15th September 2025)

3.1. RBC requests in Q1 & Q2, a total of 81 cases were received of these 7 have been completed and 18 remain outstanding and 46 cases were closed as an Invalid Request. During 2024/25 finical year the Customer Relations & Information Governance Service took over the process for dealing with requests for CCTV footage and the figures in the table below reflect these. 1 case is currently on hold – awaiting further information from the requester and 9 cases are on hold – awaiting Identification Verification and/or Consent to be provided.

3.2. BFfC requests in Q1 & Q2, a total of 57 cases were received, of these 8 have been completed and 30 remain outstanding and 11 cases were closed as an Invalid Request. 2 cases are currently on hold – awaiting further information from the requester and 6 cases are on hold – awaiting Identification Verification and/or Consent to be provided.

3.3. The implementation of the redaction software continues; we have had training on the system and has been user acceptance testing. However, the system seems to have limitations which did not present to us at the time of procurement. We have raised these concerns with the Supplier who is working in the background to correct and meet our needs. The Information Rights Services Manager is in weekly contact with the Supplier with feedback from the testing in order for them to make system improvements. The Information Rights Services Manager is also reviewing the terms of the contract with regards to a possible termination should matters not improve by the end of October 2025.

SAR Backlog Data as at 15 September 2025.

	22/23		23/24		24/25		25/26	
	RBC	**BFfC**	**RBC**	**BFfC**	**RBC**	**BFfC**	**RBC**	**BFfC**
No. Received	46	59	80	75	144	58	81	57
No. Outstanding	0	3	1	1	14	15	18	30
No. On Hold (Requires Further Info)	0	0	0	0	0	0	1	2
No. On Hold (No Consent/ID)	0	0	0	0	0	0	9	6
No. Completed	45	53	68	62	46	20	7	8
No. Declined (Invalid Request) *	1	3	11	12	84	23	46	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. ICO Guidelines.*

FOI cases

3.4. 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

3.5. Notwithstanding these measures, performance across the Council has taken time to show some improvement. Low figures have been reported to previous Committees however we reported improvements to response rates at the previous Committee in April 2025. It was subsequently discovered that in changing the method of reporting, the team had inadvertently selected an incomplete data set to report upon. This was discovered by the Performance Team on collating data for CMT. The consequence of this was that earlier cases in the period had not been counted for the stats reported to A&G.

3.6. The FOI Team (Customer Relations) and the Performance Team have reviewed the data and the process used to report data going forward. This reporting is now in accordance with the Information Commissioners Office (ICO) guidelines. We are no longer basing our response rates on the number of cases received vs number of cases responded to. But number of cases responded to vs number of cases responded to in timescale.

3.7. Tables below show the annual data for 2024/25: Total number of FOI's received by Directorate.

Directorate	**Total No. Received**
BFfC	155
DACHS	175

DEGNS	430
DoR	331
Total	1091

3.8. Tables below show the total number of FOI's responded to in 2024/25 by Directorate. 74% of the 989 cases that were responded to were responded in timescale.

Directorate	**Total Number responded to in timescale**
BFfC	135
DCASC	159
DEGNS	398
DoR	297
Total	989

3.9. The following table is the number of FOI cases received in Q1 of 25/26 for RBC and BFfC.

Directorate	**Total No Received.**
BFfC	40
DACHS	58
DEGNS	115
DoR	99
Total	312

3.10. Tables below show the total number of FOI's responded to in Q1 of 2025/26 by Directorate. 87% of the 310 cases were responded to in timescales.

Directorate	**No Responded to in timescales**
BFfC	44
DACHS	59
DEGNS	110
DoR	97
Total	310

3.11. The Information Rights Services Manager provides monthly reports in this format to the Corporate Management Team. The Customer Relations & Information Governance Service staff have worked with the CCM Project Business Analysts and the Supplier to correct the system issues, obtain regular reports, and train the organisation. The Information Rights Services Manager attends the CCM Project Borad and is kept informed of the progress of this project and tracks the issues log with the allocated Business Analysts.

3.12. With the corrections noted above and the reports in place we expected the data for Q2 to keep improving. Data for the first 2 months of Q2 is below and shows that 87.2% of the 196 responses were sent out in timescales:

3.13. **Q2 2025/26 – up to the 31st August RBC & BFfC**

Directorate	**FOI's received in Q2**	**Number responded to in Q2**
BFfC	36	28
DCASC	44	33
DEGNS	113	100
DoR	45	35
Total	238	196

3.14. The Responders whose names appear on the overdue reports are prompted/reminded by the Information Rights Services Manager, by email and via Teams, to respond in time. Emails are copied to the relevant Executive Director and Assistant Directors who also now have licences and can self-serve their information.

3.15. Of the FOI's responded to in Q1 and Q2 to date, 6 requests for Internal Review of Freedom of Information responses were received. 3 have been responded to with the Council's original response upheld and 3 are currently open with reviews in progress.

Data Transparency

3.16. The Data Transparency pages are up to date for Contracts costing over £5000 with data for quarters 1 to 2 of 2025/26 published. Expenditure over £500 for Q1 of 2025/6 is published as is the first month of Q2, July. August is currently being drafted. A revised senior management structure chart is required, to reflect recent management changes in DoR, this has been requested from the AD for HR & OD.

3.17. We have noted also that the Parking Services accounts and Parking Annual Report for 2023/24 require publishing an up-to-date report, the Parking Service has assured the Information Rights Services Manager that this task will be completed this autumn.

Information Governance Board

3.18. 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). Where any subsequent actions are identified then these are monitored.

3.19. There were 94 data related incidents reported to the Information Governance Team. One report met the criteria for notifying the ICO, disclosure via email which contained Special Category Data. The email was confirmed as deleted and not shared. The ICO recommended preventive measures, which were fed back to the respective work areas.

3.20. The main themes around the above breaches were the misdirection of emails and postal communications as a result of human error. All breaches are discussed at the

Information Governance Board where necessary specific training and improvement action plans for services are recommended.

3.21. We reinforce the messaging to the organisation around checking that the correct recipients and their addresses (email and postal) are correct before sending, we copy ICO Decision Notices along with their recommendations to Service Managers and direct staff to revisit the IG and Cyber Training following a breach.

Information Management Strategy

3.22. 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.

3.23. The Action Plan from this has since been changed to the ICO's own template, this will allow for better tracking and reporting of actions completed once work resumes with the Data Stewards.

3.24. The work with Social Care & Housing Data Stewards (BFfC and DCASC) and Corporate Data Stewards were postponed whilst resource from the Information Governance Team was allocated to an increase in business-as-usual tasks, process improvements for the Arcus system and user acceptance testing on the redaction software system.

3.25. The IG Team have created a Data Stewards site on SharePoint with access to guidance, templates and processes they require to complete work outlined in the Action Plan. The work on updating the external website to share information and ensure transparency about how the Council and BFfC work to the Data Protection Act has progressed, much of the information has been in 2025, however will not be completed until the Information Governance Officer return from long term absence.

Training

3.26. Cyber Security and Information Governance training is a mandatory requirement for RBC and BFfC staff. This is available to all staff and members through Learning Pool, the Council's e-learning package. The Senior Leadership teams within the Council and BFfC have been asked to monitor their own areas for compliance through the Power Bi reporting tool. The expectation is that SLG will be able to monitor their own staff and where there is non-compliance, they can take appropriate action to encourage their staff to complete the training. However, the Mandatory Training Task & Finish Group continue to monitor uptake and staff who have not completed the training will be given a timescale to complete the training before their system is disabled.

3.27. The content of the training suite of Cyber Security and GDPR training was revised for 2025/26 using the skills within the organisation and examples of breaches recorded within RBC and BFfC have been used as a learning tool. This inhouse suite of training was rolled out to all staff via the Learning Pool in June 2025. The table at 3.31 shows the uptake as of 09 September. The IG Team continue to provide bespoke training for colleagues without access to IT systems. Sessions were completed with Highways, Grounds personnel, and Hexagon staff.

3.28. The Mandatory Training Task & Finish Group has been working to ensure mandatory training requirements are communicated to staff, that there is appropriate monitoring and follow up to ensure that training is delivered as envisaged by CMT. The table at 3.31 shows the uptake as of 09 September, this group will continue to ensure uptake improves through weekly comms, and direct emails to staff.

Next Steps

3.29. The focus is on user acceptance training on the redaction software and commencing with the work that was started with the Data Stwerds Network. Further comms to the organisation around the importance of completeing the IG and Cyber security training.

Cyber Security Programme

3.30. This Committee requested an update around the cyber security programme, this consists of the areas of focus set out in below.

3.31. Cyber Incidents

1. Phishing -
   We continue to see more sophistication with phishing attacks majority of which are caught by our tools. However we have seen a few successful attempts where users have unwittingly clicked on links.
2. Recently we saw a phishing attack which was caused by a vulnerability in the Microsoft email exchange protocols. RBC was not the only target, and we are aware of at least one other Berkshire authority where this phishing attack was successful.
3. We continue to monitor our email exchange to keep up with these and insist users keep themselves up to date by carrying out refresher training on cyber security and GDPR.
4. A ransomware attack simulation was rehearsed by council officers in the Spring and will be rehearsed further at the Managers Teamtalk event in September 2025.
5. A cyber resilience group is being considered to help manage engagement and business continuity in the event of a cyber-attack.

3.32. Suspicious Email & Security Trends

Management Information

This report presents a consolidated record of all inbound emails that were proactively blocked by the system over the past 13 months, highlighting trends, volumes, and potential threats.

Incoming Mail Blocked

Month	Quantity	%
Jun-24	1,698,978	70.90%
Jul-24	1,320,211	64.70%
Aug-24	1,660,179	70.90%
Sep-24	1,878,700	72.30%
Oct-24	1,645,645	68.30%
Nov-24	2,129,015	74.50%
Dec-24	1,843,373	75.40%
Jan-25	3,212,538	80.70%
Feb-25	11,616,034	94.40%
Mar-25	7,595,422	90.80%
Apr-25	4,441,740	86.30%
May-25	4,405,655	86.00%
Jun-25	3,688,091	83.20%
Jul-25	3,605,594	82.70%

3.33. **Upcoming Security Changes** -

More effort is going into ensuring all applications have Multi Factor Authentication from Sept 2025.
Users will be transitioned to Microsoft Authenticator or phone verification.

3.34. **Cyber Security & IG Training Statistics:** See comments above at paragraph 3.27

Directorate	Cyber Completed	CGRP Completed
BFFC	32.5%	37.45%
DCASC	33.23%	34.42%
DEGNS	25.83%	26.00%
DOR	26.24%	27.34%

4. Contribution to strategic aims

4.1. 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”.

5. Environmental and climate implications

5.1. The Council declared a Climate Emergency at its meeting on 26 February 2019 (Minute 48 refers).

5.2. There is nothing within this report which is of relevance for the Council’s strategic priority of Climate Change.

6. Community engagement

6.1. It is not anticipated that there will be public consultation on the Information Management Strategy or Action Plan. It will however be in the public domain at Policy Committee and this Committee, and I anticipate members will wish to receive regular updates at this Committee. This will ensure that progress in this field is visible to residents.

7. Equality impact assessment

7.1. An Equality Impact Assessment (EIA) is not relevant to this report. All citizens have rights to information and there is no evidence that any section of the community is disadvantaged in accessing those rights under the current service provision. There is no reason to think that any section of society will be adversely affected by the roll-out of better Information Governance and an Information Management Strategy within the Council.

8. Other relevant considerations

8.1. Nothing relevant.

9. Legal implications

9.1. The Council is required to comply with a number of information governance regulations including the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations and the Access to Information Act. 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.

10. Financial implications

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

11. Timetable for implementation

11.1. Not applicable.

12. Background papers

12.1. There are none.