Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	15 March 2022
Title of report:	Information Governance – Update Q4, 2021/22 to date
Report by:	Lynne Ridsdale – Deputy Chief Executive
Decision Type:	For information
Ward(s) to which report relates	All

Executive Summary:

Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, ensuring compliance with the relevant statutory and regulatory requirements. At its November meeting the Audit Committee received an update on Quarter 3 activity to date.

During Quarter 4, the Council has continued to progress in responding to the ICO's recommendations, with this report updating on each of the ICO's identified actions. The report details progress to date in Quarter 4, however, further progress is expected during the remaining weeks. Where actions have responded to, these are marked as '**Complete**'. Progress against the 'urgent' actions identified by the ICO are also shown in Appendix A.

By the end of Quarter 4, the majority of the ICO's actions will be completed as planned. This will now allow a focus on Information Governance becoming one of the basic principles of the Corporate Core, as informed by the consensual audit from the ICO. This will also involve the regular reporting of Information Governance to future meetings of Audit Committee, including through corporate KPIs and breach recording and monitoring.

Key considerations

1.0 Introduction

1.1 This report is the update on Information Governance work completed to date in Quarter 4 of 2021/22.

1.2 It also demonstrates the Council's next steps in ensuring that Information Governance in embedded as one of the basic principles of the Corporate Core, as informed by the ICO's consensual audit. This will result in more concise reports in future, to focus on delivery of and performance against Information Governance requirements, including the corporate KPIs and breach recording and monitoring.

2.0 Background

2.1 The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation.

2.2 Bury Council agreed to a consensual audit by the ICO of its processing of personal data which was carried out 22nd – 24th June 2021.

2.3 The primary purpose of the audit was to provide the ICO and Bury Council with an independent opinion of the extent to which Bury Council, within the scope of the agreed audit, is complying with data protection legislation.

2.4 A report has been provided to Bury Council which, along with a series of recommended actions, also reflected on areas of good practice.

2.5 Since the provision of the ICO's report, Bury Council has developed a detailed workplan to respond to the issues raised.

2.6 This report provides Audit Committee with the regular update of the Council's progress against this workplan.

2.7 Future reports will focus on the Council's delivery of information governance, as an embedded part of ongoing service delivery.

3.0 Improvement Plan

3.1 The ICO made 79 recommendations across the three themes of the audit, which have also been categorised by level of priority as follows:

	Urgent	High	Medium	Low	Total
Governance and Assurance	7	15	14	2	38
Information Security	-	5	18	8	31
Freedom of Information	-	4	5	1	10

3.2 Appendix A provides details of progress against the 7 'urgent' recommendations identified by the ICO.

3.3 The recommendations have been translated into a detailed improvement plan for delivery by the end of the 2021/22 financial year. The detailed plan, which is performance managed by the Information Governance Steering Group, is attached for information. A synopsis of activity initially planned is as follows:

By end August	• Resolve Legitimate Interest Assessment – HR • ROPA refreshed • Review responsibilities/resources for IG • Refresh & re-establish network IG champions • Risk management strategy approved • Individual rights policy & procedure drafted • IG Policies updated to reflect GDPR • Induction updated & systems access only granted once e-learning complete • Contacts reviewed re data processing • DPIA screening, template and log established
By end Sept	• Resolve IS responsibilities within ICT • Update agile policy re information security • PEN test and review PSN requirements • Update personal breach policy • policy document template & schedule approved, including Information Security • policy availability to non-front line staff addressed • IG KPIs reviewed • IAR reviewed following ROPA refresh • ROPA review process agreed • Privacy notice log established • FOIA policy and procedure updated
By end Oct	• Review GDPR e-learning module • Update Information Security policy in full • Establish end use asset register • Port controls designed within Enterprise Agreement

	• Specialist role training delivered to IG leadership roles • Internal audit plan
By end Nov	• Process for reviewing systems access in place • Resolve information security within buildings including floor walks of office sites
By end Dec	• End user device policy in place • Starter/leavers process reviewed and induction updated • Plans in place for independent assurance of IG • Audit of consent processes and recording • Review PETS

4.0 Information Governance Update 2021/22 Quarter 4 to date

4.1 The following updates are provided against activity which is scheduled for completion at this point within the overall work programme:

- Resolve Legitimate Interest Assessment – HR
  - **Complete**. The assessment concluded a legally acceptable basis on which employee personal information is processed and stored as HR's activities do not override individual rights.

- ROPA refreshed
  - **Complete**d by all departments. Follow up meetings with individual managers / services are currently being held to review the ROPA responses provide, and subsequently to make any further updates and additions. Follow up meetings with individual managers / services have commenced to review and update responses, including any associated data records of DPIAs, DSAs, Privacy Notices, etc.

- Review responsibilities/resources for IG
  - **Complete**. Dedicated Information Governance Manager and Data Protection Officer post created and filled. Additional project resource in place to deliver the improvement plan on a fixed term basis

- Refresh & re-establish network IG Champions
  - **Complete**. Nominations received from teams and services, with 37 volunteers obtained to date. Initial meeting of the Champions held at the start of December to highlight role and expectations. Programme of bi-monthly meetings established.

- Risk management strategy approved

- **Complete**. An IG Risk Register developed. This will ensure that all areas of concern or risk relating to IG matters will be monitored and addressed in a timely manner. This document is reported to the IGSG on a monthly basis, with any changes or additions highlighted.
-

- Individual rights policy & procedure drafted
  - **Complete.** This policy has been revised and approved by the IGSG.

- IG Policies updated to reflect GDPR
  - **Complete**. The following policies have all been revised and approved by IGSG:
    - Appropriate Policy Processing Special Category Data
    - Data Processing Impact Assessment
    - GDPR – Legitimate Interests Template
    - Data Breach Reporting
    - Data Processor Agreement
    - Data Quality Policy
    - Data Sharing Agreement
    - Data Sharing Guide
    - Data Subject Rights Policy
    - Environmental Information Regulations Procedure
    - Freedom of Information Requests Procedure
    - Information Governance Complaints Procedure
    - Information Asset Owner, Information Asset Manager & Information Asset Administrator Responsibilities
    - Privacy Notice Template
    - Subject Access Requests Procedure

- Induction updated & systems access only granted once e-learning complete
  - **Complete**. Onboarding processes revised to ensure ICT access only granted once IG e-learning complete. Learning to be completed within first 5 days of commencement of employment.
  - Process in place to identify new starters and to remove ICT access if training not completed.

- Contracts reviewed re data processing
  - **Complete** - A spot-check review of existing contracts valued at under £75,000 has been undertaken in collaboration with Procurement. These have been identified to pose the highest risk of non-compliance to data protection legislation, as those at a greater value must undergo a robust process before engagement. The Corporate Contracts Register will now include information as to if the contract involves the processing of personal data and relevant information governance mechanisms have been applied. This will be reviewed by the Information Governance Manager on an annual

basis and progress reported to IGSG quarterly. A Data Processing Agreement containing appropriate IG clauses has been drafted by Legal and approved for appending to existing contracts as required. Invitation to Tender, Request for Quotation and Privacy Notice – Council Purchasing Cards have also been reviewed and strengthened the implementation of good Information Governance practices when engaging third party suppliers.

- DPIA screening, template and log established
  - **Complete.** Policy and template revised and approved by IGSG. Log included in the ROPA.

- Resolve IS responsibilities within ICT
  - Ongoing. IS policies reviewed. Work ongoing to revise IS policies, which will also include new components of Microsoft 365. Work due to complete by end of March 2022.

- Update agile policy re information security
  - Ongoing. Currently under review with all IS policies. Work expected to be complete by end March 2022.

- PEN test and review PSN requirements
  - Ongoing. Timetable revised to test in December to align with activities in ICT calendar. PEN test was completed in December as per schedule. A list of remediation activities has been agreed prior to submission of the next application for PSN accreditation. A number of these activities are linked to the Cloud Migration project and moving key line of business systems off old servers. A plan is being agreed with services with moves taking place until the end of April. The application for a new PSN certificate will be made by the end of February.

- Update personal breach policy
  - **Complete.** Policy reviewed and approved by IGSG.

- Policy document template & schedule approved, including Information Security
  - **Complete**. Template applied to all policies in development

- Policy availability to non-front-line staff addressed
  - Ongoing. Requirement with internal communications for response. All staff will have a Council email by the new financial year; policy access will be available from that time. All policies will be made available for staff / customers via the intranet / internet now approved by IGSG.

- IG KPIs reviewed
  - **Complete**. Corporate Plan PIs have been updated to include number of complaints and number data breaches. Information reported on FOIs and

SARs completed in time are reported against the Business Excellence Transformation theme in the first performance report against the Bury Council and CCG integrated Corporate Plan. Performance against indicators to be reported to Information Governance Steering Group on a monthly basis and Audit Committee on a quarterly basis.
    - Suite to be strengthen after review of best practice in other organisations.

- IAR reviewed following ROPA refresh
    - Ongoing. Information Asset Register (IAR) to be reviewed following ROPA refresh and follow-up meetings planned for February – May 2022.

- ROPA review process agreed
    - **Complete**. Programme of spot-checks developed for annual review on completion of all ROPA-related work. A rolling review of ROPA entries will be introduced with regular updates to each meeting of the Information Governance Steering Group. Additional column added to ROPA spreadsheet to include details of any associated contracts.

- Privacy notice log established
    - **Complete**. Privacy notices included in ROPA.

- FOIA policy and procedure updated
    - **Complete**. Policy reviewed and approved by IGSG.

- Review GDPR e-learning module
    - **Complete**. Alternative E-Learning modules within the existing training platform covering Information Governance and Cyber Security have been reviewed against National Cyber Security and ICO guidance and assurance provided they meet requirements of the audit recommendations.
    - New Data Breach module and test developed internally.
    - New suite of training developed to cover the issues raised by the ICO. This now includes courses on GDPR, FOI, Cyber Security, and Data Breach process, together with overall Quiz developed.
    - Overall pass mark of 80% required for all staff.
    - All new starters, those required to repeat training after making data breach or on annual refresh of training will complete new training modules.
    - Reminders to refresh training will be sent to all staff one month prior to one year anniversary of completion.
    - Training now focused on 'paper-based' module for non-office based staff.

- Update Information Security policy in full
    - Ongoing. Information Security Policies currently being reviewed as part of IG Policy review. Initial review completed, with revised document scheduled for completion by end of March 2022.

- Establish end use asset register
    - Ongoing. To be developed following review of IS policies and linked to ROPA.

- Specialist role training delivered to IG leadership roles
    - Ongoing. SIRO training complete. Training for IG Manager to be developed and arranged. Further training programmes for senior Council officers identified and being developed.

- Internal audit plan
    - **Complete**. Recommendations incorporated into IG Workplan.
    - Revised and updated version of Workplan included as Appendix 1.

- Process for reviewing systems access in place
    - **Complete**. All staff with access to ICT systems have completed and met pass-mark for online IG training. Access to systems removed from officers not successfully completing training.

- Resolve information security within buildings including floor walks of office sites
    - Ongoing. To be included in revised IS policy to be completed March 2022. Floor walks commenced January 2022.

- End user device policy in place
    - Ongoing. To be included in IS policy review to be completed March 2022.

- Starter / leavers process reviewed and induction updated
    - **Complete**. All new starters required to complete new IG training suite within first five days of starting or access to systems removed.

- Plans in place for independent assurance of IG
    - **Complete**. Progress reviewed by Mazars in February 2022. Additionally, completion of the DSPT later in 2022 will provide this external challenge and review.

- Audit of consent processes and recording
    - Ongoing. To be concluded with review of IS policy.

- Review PETS (Privacy Enhancing Technologies)
    - Ongoing. To be included in the IS policy review to be completed March 2022.

By the end of Quarter 4, all of the ICO's recommendations will be largely completed, with the remaining actions due for imminent completion. This will allow a refocus from

response to the ICO's recommendations to information governance becoming one of the basic principles of the Corporate Core.

4.2 Managing Data Breaches

In addition to the scheduled work plan, Data Breach monitoring and review has increased, with increased challenge to remedial actions taken by teams coming from the Information Governance Manager and DPO. Advisory letters sent to all officers responsible for a data breach to make them aware of implications. Officers also required to attend meetings with their Executive Director and the DPO to identify any learning or additional support needs. Officers also required to repeat the Council's online IG training module.

The majority of breaches are due to correspondence being sent to incorrect recipients, either by post or email. Key learning from these breaches has been for officers to take more time when sending out information and to double check addresses used before sending. Officers are also recommended to use the 'delay' facility in Outlook to allow messages to be rechecked after 'send' button used. Officers also reminded not to rely on 'recall' facility, especially with externally sent emails.

A presentation on preventing and reporting data breaches has been developed and offered to all teams within the Council. A good level of take up has been achieved, with particular interest coming from nearly all teams who have recently reported a data breach.

A new training model on Data Breaches and overall Information Security Quiz, requiring an 80% pass rate, has been developed and is now in use.

For the period November 2021 to March 2022, the following breaches have been recorded by department:

	BGI	CC	CC-Finance	CYP	OCO	Ops	**TOTAL**	COMMENTS
November	0	3	2	3	7	1	**16**	All except three breaches involved information sent to wrong recipient Three reported to ICO – recommendations received and matters closed
December	0	2	4	5	1	1	**13**	All except four breaches involved information sent to wrong recipient One reported to ICO – recommendation received and matter closed
January	1	1	3	3	1	0	**9**	All involved information sent to wrong recipient None reported to ICO
February	0	1	0	0	4	0	**5**	All except one breach involved information sent to wrong recipient One reported to ICO – awaiting response
March	0	0	0	1	1	0	**2**	Both involved information sent to wrong recipient
TOTAL	**1**	**7**	**9**	**12**	**14**	**2**	**45**	

5.0 Recommendations and Next Steps

5.1 The Audit Committee is required to note the 2021/22 Quarter 4 (to date) Update provided.

5.2 As noted above, by the end of Quarter 4 the ICO's recommendations will be largely complete and information governance will be an integral part of 'business as usual'. Therefore, Audit Committee is asked to note that future reports will be shorter and more focussed on updates of the Council's performance, such as against the Corporate KPIs and breach recording and monitoring.

Other alternative options considered

None.

Community impact / Contribution to the Bury 2030 Strategy

Good Information Governance practices enables the Council to deliver its statutory requirements and therefore contributes across all the themes of the Bury 2030 Strategy.

Equality Impact and considerations:

24. *Under section 149 of the Equality Act 2010, the 'general duty' on public authorities is set out as follows:*

A public authority must, in the exercise of its functions, have due regard to the need to -

(a) *eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;*

(b) *advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;*

(c) *foster good relations between persons who share a relevant protected characteristic and persons who do not share it.*

25. *The public sector equality duty (specific duty) requires us to consider how we can positively contribute to the advancement of equality and good relations, and demonstrate that we are paying 'due regard' in our decision making in the design of policies and in the delivery of services*.

Assessment of Risk:

The following risks apply to the decision:

Risk / opportunity	Mitigation
Without a robust framework in place to support good Information Governance practice, there is a risk that the Council may not comply with the duties set out in the UK General Data Protection Regulations (GDPR) or Data Protection Act leading to possible data breaches, loss of public confidence, reputational damage and prosecution / fines by the Information Commissioner	Approval and Implement of the Information Governance Framework Implementation of a comprehensive Information Governance work programme

Consultation: N/a

Legal Implications:

The report references the Council's statutory duties and obligations under the UK GDPR, Data protection Act 2018, FOIA and associated legislation and guidance. The Council has duties under this legislation in terms of accountability and compliance and must ensure it has appropriate policies and procedures in place. A failure to ensure compliance could result in enforcement action by the ICO.

Legal advice and support will be required in terms of the action plan outlined in the report as well as ongoing DPO oversight and support.

Financial Implications:

With the exception of the procurement of appropriate training there are no direct financial implications arising from this report. However, there are implications in relation to a potential ICO fine if the Council had a data breach and the ICO found that we as an organisation were negligent.

Report Author and Contact Details:

Lynne Ridsdale – Deputy Chief Executive

l.ridsdale@bury.gov.uk

Background papers:

Report to Audit Committee - Information Governance – ICO Update & Q2 delivery Update – 30 September 2021
Report to Audit Committee – Information Governance – Update Q3, 2021/22 to date – 25 November 2021

Please include a glossary of terms, abbreviations and acronyms used in this report.

Term	Meaning
BGI	Business Growth and Investment
CC	Corporate Core
CC-Finance	Corporate Core Finance
CYP	Children and Young People
DFM	Data Flow Mapping
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
FOIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulations 2018
IAM	Information Asset Manager
IAO	Information Asset Owner
IAR	Information Asset Registers
ICT	Information Communication and Technology

IG	Information Governance
IGSG	Information Governance Steering Group
OCO	One Commissioning Organisation
Ops	Operations
NHS	National Health Service
ROPA	Record of Processing activity
SAR	Subject Access Request
SIRO	Senior Information Risk Officer