Classification Open	Item No.

Meeting:	Audit Committee
Meeting date:	25 November 2021
Title of report:	Information Governance – Update Q3, 2021/22 to date
Report by:	Lynne Ridsdale – Deputy Chief Executive
Decision Type:	
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 last meeting the Audit Committee received the Q2 update on IG activity and approved the Information Governance Framework through which these functions are discharged within the Council.

During Q3 to date the Council has continued to progress in responding to the Information Commissioner's Officer's (ICO's) recommendations. This report provides an update on progress against the Information Governance workplan for Quarter 3 to date.

Prior to the ICO's visit, a review of the Council's position in relation to IG was undertaken by the Council's Internal Audit. The key recommendations of their report were similar to those made by the ICO. A review of progress against all the recommendations from Internal Audit are also shown.

Key considerations

1.0 Introduction

1.1 This report is the update on Information Governance work completed to date in Quarter 3 of 2021/22.

2.0 Background

2.1 The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation. Article 58(1) of the UK General Data Protection Regulation (UK GDPR) states that the Information Commissioner's Office (ICO) has the power to carry out investigations in the form of data protection audits. Section 129 of the Data Protection Act 2018 (DPA 18) also provides provision to carry out consensual audits. Additionally, Section 146 of the DPA 18 allows the ICO, through a written "assessment notice", to carry out an assessment of compliance with the data protection legislation.

2.2 Bury Council agreed to a consensual audit by the ICO of its processing of personal data. This was originally scheduled for June 2020; however, this was paused in response to the Covid-19 pandemic and was subsequently re-scheduled for 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. Progress against the items in the workplan is detailed below.

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 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 available for inspection. 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 of 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 Information Security (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 Key Performance Indicators (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, including port controls designed within Enterprise Agreement • Establish end use asset register • 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 3 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
  - Completed by all departments. Follow up meetings with individual managers / services are currently being held to review the ROPA responses provided, and subsequently to make any further updates and additions. Plan to be developed for spot checks to take place on regular basis.

- 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 14 volunteers obtained to date. Gaps identified will be filled by line managers. Initial meeting of the Champions to be arranged for start of December to highlight role and expectations.

- Risk management strategy approved
  - Complete. An IG Risk Register has been 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 will also be reported to the IGSG on a monthly basis.

- Individual rights policy & procedure drafted
  - At final draft stage subject to review from Head of Legal Services.

- IG Policies updated to reflect GDPR
  - The following policies and procedures have all been revised and are at final draft stage subject to review by Head of Legal Services:

        - FOI and EIR Policy
        - FOI and EIR Public Interest Test (PIT)
        - Bury Privacy Notice Template.
        - Data Subject Rights.
        - Bury IG Complaints Procedure.
        - Data Quality Policy.
    - All remaining policies and procedures will be completed by end of November for review by Head of Legal Services:
        - Appropriate Policy Processing Special Category Data
        - Anonymisation and Pseudonymisation Policy
        - Information Asset Owner and Information Asset Administrator Responsibilities

- 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.

- Contracts reviewed re data processing
    - Ongoing. A spot-check review of existing contracts valued at under £75,000 is being 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. A Data Processing Agreement containing appropriate IG clauses has been drafted by Legal and approved for appending to existing contracts as required.

- DPIA screening checklist, full assessment template and log established
    - Policy and template reviewed and awaiting approval from Legal. Log to be established by end of November.

- Resolve Information Security (IS) responsibilities within ICT
    - IS policies to be reviewed with all IG policies by the end of November. This will highlight any issues for clarification.

- Update agile policy re information security
    - To be reviewed with other IG related policies by end of November.

- PEN test and review PSN requirements
    - Ongoing. Timetable revised to test in December to align with activities in ICT calendar. External element of the PEN test (a simulated and authorised cyberattack on a computer system to evaluate the security of the system) due to complete November. Internal tests to commence and complete December.

- Update personal breach policy
    - At final draft stage subject to review from Head of Legal Services.

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

- Policy availability to non-front-line staff addressed
    - 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 once approved.

- IG KPIs reviewed
    - Complete. Corporate Plan PIs have been updated to include a number of complaints and 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, Quarter 3, 2020/21. Performance against indicators to be reported to Information Governance Steering Group monthly, and Audit Committee on a quarterly basis.
    - Suite to be strengthened after review of best practice in other organisations.

- Information Asset Register (IAR) to be reviewed following ROPA refresh
    - Completion of IAR moved to December on completion of ROPA follow up meetings, when full picture of all assets will be known.

- ROPA review process agreed
    - Programme of spot-checks to be developed 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
    - At final draft stage subject to review from Head of Legal Services.

- Review GDPR e-learning module
    - 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 of GDPR, FOI, Cyber Security, and Data

    - Breach process, together with overall Quiz developed.
    - Overall pass mark of 80% required for all staff.
    - Currently being reviewed prior to wider launch.
    - Launch will focus on new starters and those who have not yet completed training.
    - Approximately one month before twelve months expire since last completion of training, reminders will be sent to all staff. This is likely to be May 2022 and linked to suggested IG awareness month of communications.

- Update Information Security policy in full, including port controls designed within Enterprise Agreement
    - Information Security Policies currently being reviewed as part of IG Policy review. Due to complete by November, to then be reviewed by Head of Legal Services.

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

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

- Internal audit plan
    - Recommendations incorporated into IG Workplan.
    - Details of actions taken and tasks completed detailed in section 4.3 below.

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 Team and DPO.

A presentation on preventing and reporting data breaches has been developed and offered to all teams within the Council. A high 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 undergoing final amendments and testing before formal launching of the new IG E-learning Suite.

All officers making a data breach will be required to repeat the Council's training module, and will receive a letter from the Data Protection Officer to make them aware of the severity of breach and the risks to the Council and themselves; they will also meet with their Executive Director to discuss the matter and identify any further support which they might require.

4.3 Response to Internal Audit recommendations

The overall findings of the Internal Audit rated the Council as 'Moderate Risk' with respect to its approach to IG. However, 15 recommendations were identified needing 'Significant' attention, with a further 9 that were deemed to 'Merit Attention'. The key risks are shown (in bold) below, along with the specific recommendations made where action needs to be taken and the Council's current response:

1. **Risk GDPR Legislation is not complied with and the Council may be subjected to financial penalties. The Council does not control the information it holds.**

1.1 All departments should be required to update and confirm the accuracy of the ROPA (Significant)

- Complete. All departments have provided updates for the ROPA. These are currently being individually reviewed with members of the IG Team.

1.2 All departments should be required to confirm that privacy notices are in place for all systems that process personal data (Significant)

- Complete. This information is included in the ROPA.

1.3 Personal data audits should be undertaken across all services to clarify all data flows. (Significant)

- To commence on completion of all ROPA follow up meetings.

1.4 There should be a corporate approach to the management of ongoing consent to provide assurance to the Council that information held is permitted, accurate and up to date. It should be established if individual system owners have any processes in place for managing ongoing consent, the processes should be review and checked to ensure they comply with guidance. Additionally, it should be established whether Department / Systems Owners maintain records of requests to dispose of personal data and if so if these requests are held securely and have been actioned in a secure manner. (Merits Attention)

- To be addressed on completion of the IG / IS policy review.

1.5 The Council should undertake the three-part test to demonstrate it has fully considered and protected individuals rights and interests. (Merits Attention)

- To be developed as part of the IG / IS policy review.

1.6 Procedures should be introduced to ensure that the records retention schedules in each department are reviewed and updated periodically.

(Merits Attention)

- To be developed on completion of the follow up ROPA activity.

1.7 In the event of staff returning to work in the administrative buildings, management should consider introducing cross shredders across the council to enable the prompt disposal of confidential waste. Guidance also needs to be issued to staff working at home on sage disposal procedures for confidential waste. This should be incorporated into corporate homes working policies and procedures. In additional, all Council officers should be encouraging to reduce the use of paper documents. (Merits Attention)

- To be incorporated into the IG / IS policy review.
- Walk round of offices to be carried out on a routine basis to ensure compliance.
- Weekly comms to remind staff in offices and agile working of the need to dispose of documents appropriately.

2. **Individuals' Rights are Not considered in process activities**.

2.1 The individual system privacy notices should be reviewed to ensure that they are consistent and provide all the information as required by the GDPR legislation (Significant)

- Complete. Record of privacy notices included in the ROPA.

2.2 A Corporate approach to handling SARS / FOIs should be introduced and implemented as soon as possible. Staff undertaking enquiries to address SAR / FOI requests should be provided with training to ensure that all requests are dealt with appropriately and in a consistent manner, with Senior Management being required to sign off responses before they are issues (Significant)

- Process to be included as part of the IG policy review.

3. **The Council has no governance arrangement for ensuring data is protected**.

3.1 The Communities and Wellbeing (NB no longer exists) and Corporate Core departments should ensure there is appropriate representation on the IG group. The group meeting should be resurrected to ensure that the profiles of GDPR is still high on the agenda and to ensure that compliance with GDPR legislation continues to be addressed. (Significant)

- Complete. IG Steering Group contains representation from all departments.
- IG Champions network being established to ensure involvement and ownership at all levels of the organisation.

3.2 Clearly defined roles and responsibilities need to be established for the on-going management of GDPR. Once these are established, this information should be disseminated to Business Managers and staff. (Significant)

- Complete. SIRO and IG Manager / DPO identified. Support from key senior managers identified via the IG Steering Group.

3.3 The IG Group should be encouraged to develop its protocols to ensure that information is effectively disseminated to business managers across the council. (Significant)

- Complete – IG Steering Group to own all IG related tasks.
- Complete – weekly IG communications issued to all staff.
- IG Champions network being established.

3.4a Consideration should be given to mandating a clear desk / clear wall policy in all administrative buildings to ensure that all business sensitive / personal information is not left in a place where the information could be compromised. Guidance needs to be developed for all staff working at home to ensure that Council data is kept secure. (Significant)

- To be developed as part of policy review.
- Message to be cascaded via weekly IG Communications.
- Walk-rounds of offices to commence on approval of policies.

3.4b All staff who work in the administrative buildings should be reminded on the need to maintain security regarding data and should be encouraged to challenge anyone that is not wearing an ID badge and / or acting in a suspicious manner. (Significant)

- Reminder to be included in weekly IG Communications.

3.4 The latest version of the Data Protection Policy should be published on the intranet / internet, so it is available to staff / public. (Merits Attention)

- To be completed on formal approval of revised policies.

3.5 GDPR compliance checks should be undertaken on a period basis to ensure compliance is maintained. Consideration also needs to be given to how compliance will be maintained with staff working from home on a permanent basis. (Merits Attention)

- To be developed in New Year on completion of policies review.

4. **Staff have not received training on GDPR and are not following the principles**.

4.1 Managers should be reminded of the need for all members of staff to complete the GDPR online training module and a date for all staff should be set. (Significant)

- Complete. During Summer 2021, all staff required to repeat training.
- Annual reminder to be issued by IG Manager.
- Process being finalised for all new starters to complete training within first 5 days of employment to obtain access to systems.

5. **The Council does not have contracts in place with data processors and is unaware how Council information will be handled by 3rd parties.**

5.1 System owners should be reminded of the need to ensure that there are written agreements in place for all data that is processed by outside parties (Significant)

- Ongoing. Spot-check review of existing contracts valued at under £75,000 is being 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. A Data Processing Agreement containing appropriate IG clauses has been drafted by Legal and approved for appending to existing contracts as required.

5.2 The Council should review its Project Initiation Document to ensure that appropriate DP measures are incorporated into any system developments (Merits Attention)

- Complete. All policies now use this format.

6. **Data Protection privacy impact assessments are not undertaken**.

6.1 All system owners should be required to complete a Data Protection Impact Assessment to provide assurance to the Council that all risks have been identified. (Significant)

- Complete. Part of ROPA.

7. **Data Security, International Transfers and Breaches**

7.1 The Council's ICT Security should be reviewed and updated to reflect the current GDPR / DP legislation. The revised document should be circulated so all staff are again made aware of GDPR requirements. (Significant)

- To be included in review of all IG / IS policies. Due for completion end of November.

7.2 All staff should be reminded that confidential data should not be sent outside the council IT network to personal email accounts. Management should consider further compliance checks to ensure that personal data is not being sent to employees' personal email accounts. (Significant)

- Complete. Weekly IG Communications informed all staff of need to use Egress system when sending personal data outside the organisation.

7.3 The Paper Records and Data handline and Transit policy should be reviewed, and all staff should be encouraged to work in a paperless environment. The policy will need to be updated to reflect the arrangement for staff working from home. The policy should then be relaunched to all staff. (Significant)

- Included in review of all IG / IS policies.

7.4 The personal Data Breach Reporting Policy should be updated with the current DP Lead's contact information. In addition, the record of all data breaches should be forwarded to Internal Audit for review (Merits Attention)

- Complete. Awaiting input from Head of Legal Services and formal approval.

5 Recommendations

5.1 The Audit Committee is required to note the 2021/22 Quarter 3 Update provided.

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

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

Term	Meaning
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
ICO	Information Commissioner's Office
ICT	Information Communication and Technology
IG	Information Governance
IGSG	Information Governance Steering Group
IS	Information Security
NHS	National Health Service
PSN	Public Services Network

ROPA	Record of Processing activity
SAR	Subject Access Request
SIRO	Senior Information Risk Officer