Information Governance Incident (Data Breach) Procedure

Author: Rachel Everitt

Date: September 2024

Version: v2.0

Title	Information Governance Incident Procedure
Author	**Data Protection Officer**
Owner	**Data Protection Officer**
Created	**March 2022**
Approved by	**Audit Committee**
Date of Approval	**February 2005**
Review Date	**February 2027**

Document Version Control

Document Version Control	
Issue Number	Date
1.0	March 2022 (Bury Council)
2.0	September 2024

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

1. Introduction

What is an Information Governance Incident

An Information Governance Incident, or data breach, occurs when there is an accidental or deliberate breach of security leading to:

- The accidental or unlawful destruction of personal data,
- Loss or alteration of personal dataUnauthorised disclosure of, or access to personal data, transmitted, stored or otherwise processed

Some examples of incidents include (but are not limited to):

- Staff accessing records on case management systems where they have no business requirement to view (unauthorised access)
- Personal data sent to the wrong recipient in error (human error)
- Loss of paperwork containing personal data
- Loss of availability of personal data (lost paperwork, equipment failure)
- Successful hacking attacks
- Poor disposal of confidential waste (not cross shredded or placed in the secure confidential waste bin)

A personal data breach will occur whenever personal data is lost, destroyed, corrupted, disclosed, or accessed without authorisation. Bury Council is required to record and manage all incidents and near misses.

An Information Governance Incident involving personal information is likely to constitute a breach of the UK General Data Protection Regulation ('UK GDPR') and the Data Protection Act 2018.

How to manage an information incident

There are four elements to the information incident management process

- Containment, escalation and recovery;
- Assessment of on-going risk;
- Notification;
- Evaluation and response.

The UK GDPR places a requirement on all organisations to report certain types of data breaches to the regulatory authority (ICO – Information Commissioner's Office), and where necessary inform the individuals affected by the breach.

Bury Council has a duty to report the breaches caught in this requirement to the ICO within 72 hours of becoming aware of the breach. The 72 hours includes evenings, weekends and bank holidays so it is imperative that all incidents are reported as soon as we become aware of them.

This procedure is part of Bury Council's Information Governance Framework and should be read in conjunction with the other policies and procedures within the framework.

Scope

This policy applies to all Bury Council employees, seconded staff members, temporary staff, councillors, volunteer and third-party contractors.

2. Managing an information governance incident – Stage 1

Containment, escalation, and recovery

Every employee within Bury Council is required to report any information governance incident immediately to the following;

1. Your line manager or next available manager if they are unavailable.

2. The Policy Compliance Team via emailing; **ig@bury.gov.uk**
    - The Policy Compliance Team will log the incident, provide the information security breach form with incident number for completion by the investigating officer and give advice on any immediate action required to contain the incident. The incident form

can also be obtained from the Information Governance intranet page.

- Heads of Service (Information Asset Owners) and Managers (Information Asset Managers) must also be made aware of this incident immediately.
- The incident form with initial investigation to be returned to the Policy Compliance Team at the earliest opportunity, but no more than 24 hours of the breach being discovered, regardless as to if this falls on a working day or not. This allows the Policy Compliance Team to determine whether or not the breach is reportable and if so, **notify the Information Commissioner's Office (ICO) within the 72 hour statutory time frame**.
  The Caldicott Guardian (where appropriate).

3. Contact ICT if any ICT equipment, system or website is involved in the incident via ServDesk@bury.gov.uk. If an incident occurs out of hours, this should be reported to the Emergency Control Room (0161 253 6606) who will refer the call to the ICT out of hours contact.

Line managers of staff involved in the data breach must conduct a full investigation, completing the Information Security Breach form (Appendix 1) and submitting it to the Policy Compliance Team. The investigating officer must obtain all of the facts regarding the incident, recover the personal data (where able), and record any key facts/decisions made from this point forward.

The investigating officer will also need to establish whether anything can be done to recover the data and limit the damage the breach of security can cause. This might include:

- physical recovery of equipment;
- physical recovery of paperwork, where possible (this could include arranging to collect information in person or obtaining written confirmation that the information has been securely destroyed);
- use of backups to restore lost or damaged data;

- alerting staff in the area where the breach occurred, to enable them to recognise when someone tries to use stolen data to access accounts or services; or
- If there is potential for a significant impact or reputational damage the Communications team should be informed by emailing CommunicationsTeam@Bury.gov.uk.

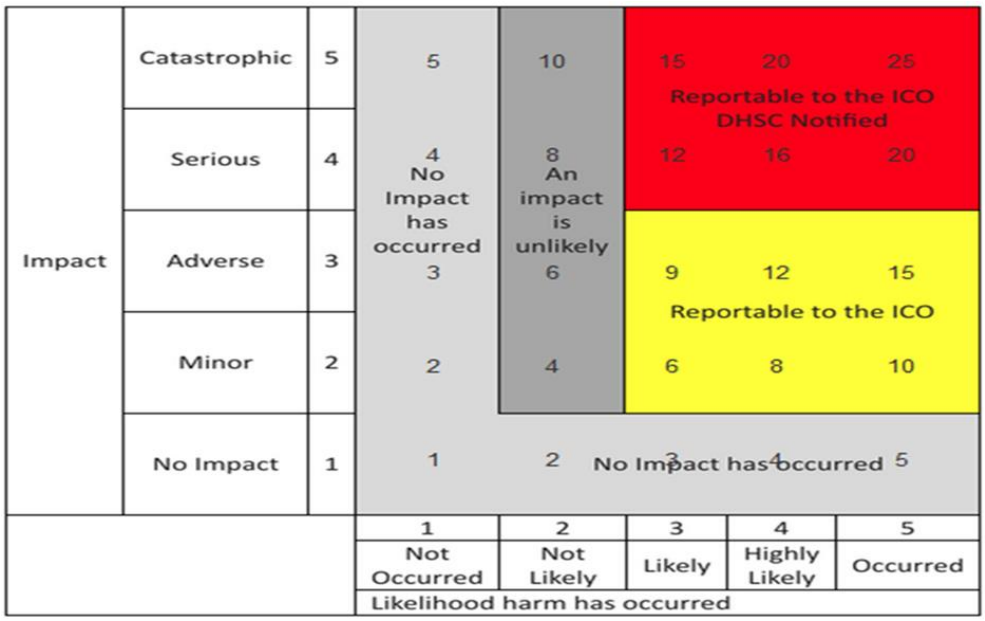
Data Security Incidents can have detrimental effects on the rights and freedoms of the individuals involved (data subject), e.g. financial information or information which indicates they are vulnerable in some way. Where any risk to the data subject is identified immediate notification should be considered.

Risks from Incidents

All risks as a result of the breach must be captured within the breach form by the line manager with the officer involved with the breach. This form to be assessed by the line manager (and then by the Policy Compliance Team) to enable Bury Council to control and mitigate any risks.

The line manager must, using the assessment grid below, determine the likelihood of harm and impact to individuals to enable the Policy Compliance Team to make the decision on whether a breach needs to be reported to the Information Commissioner's Office.

The incident must be risk assessed using the NHS Digital (HSCIC) Scale & Sensitivity Factors below. This assessment includes the number of individuals affected, type of incident, potential reputational damage, media interest and potential litigation.



The likelihood of the negative consequences occurring are graded on a scale of 1-5. 1 being a non-occurrence and 5 indicating that it has occurred.

Number	Likelihood	Description
1.	No likelihood of occurrence	There is absolute certainty that there can be no likelihood of adverse effects. This may involve a laptop encryption or reference number identification only.
2.	Not likely or any incident involving vulnerable groups even if no adverse effect occurred.	In cases where there is very limited personal data involved, or no evidence that can prove that no adverse effect has occurred, this must be selected, e.g. name or email address. Or if all the data was recovered with limited known access.
3.	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4.	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.

5.	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

The impact/severity is further graded rating the incident on a scale of 1 to 5. 1 being the lowest and 5 the highest.

Grade the potential severity of the adverse effect on individuals

Number.	**Effect**	**Description**
1.	No impact	There is absolute certainty that no adverse effect can arise from the breach – no impact
2.	Minor	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred A minor adverse effect must be selected where there is no absolute certainty.
3.	Adverse	Potentially some adverse effect. An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job.
4.	Serious	Potentially pain and suffering/financial loss There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Examples include loss of bank details leading to loss of funds. Or if there is a loss of employment. SIRO
5.	Catastrophic	A person dies or suffers a catastrophic occurrence SIRO

Where the incident is assessed that it is (at least) likely that some harm has occurred and the impact is (at least) minor, the incident is reportable.

Sensitivity factors

Sensitivity factors have been incorporated into the grading scores. If a breach involves certain categories of /sensitive data or vulnerable groups it must be assessed as at least:

- A likelihood score of 'Not likely' or 'incident involved vulnerable groups (where no adverse effect occurred)', choose 'Not Likely' on the grid;

  AND

- A severity score of 'Potentially some minor adverse effect' or 'any incident involving vulnerable groups even if no adverse effect occurred' choose Minor on the grid.

So even where an incident involves special categories/sensitive data or/vulnerable groups, on the breach assessment grid above it would be a minimum of 4 and so would not always be reportable to the ICO/ DHSC (Department of Health and Social Care). It would be reportable if the Likelihood of harm is assessed as at least "Likely"

Assessing risk to the individuals involved (likelihood)

The UK GDPR gives interpretation as to what might constitute a high risk to individuals. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

For clarity special categories or sensitive types of data under UK GDPR are:

- racial or ethnic origin,
- political opinions,
- religious opinions,
- trade union membership,
- and the processing of genetic data,
- biometric data for uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation.

Data involving the following are also to be considered as special categories or sensitive for the purposes of the risk analysis:

- vulnerable children
- vulnerable adults
- criminal convictions
- special characteristics listed in the Equality Act 2010

Containment actions can be taken which remove the need for notification to outside bodies. The DPO will make a determination on whether such circumstances apply once the form is received and reviewed by the IG Manager.

Please note that the Investigating Officer is not to report any incident to the Information Commissioner's Office (ICO)/Department for Health and Social Care (DHSC). This is to be done via the Policy Compliance Team and Data Protection Officer.

Notification to Individuals

If the breach is likely to result in a high risk of adversely affecting individuals, the relevant service may be required to inform those individuals without undue delay. This is a decision which will be made by the DPO and instructions provided by the Policy Compliance Team. The corporate template letter for contacting individuals whose data has been breached must be used.

Depending on the incident there may also be other legal, contractual or sector-specific requirements to notify various parties. Instructions to this effect will be provided by the Policy Compliance Team once a full review of the incident has taken place.

When deciding whether or not to notify individuals, consequences for the individuals must be considered, such as;

- What are the potential effects of a breach on individuals;
- How severe are these, and how likely are they to happen?

To assess 'high risk' both the severity of the potential or actual impact on individuals, and the likelihood of this occurring due to the data breach needs to be considered. In such cases, the service will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. The service must, therefore, contact the Policy Compliance Team for guidance immediately upon being aware that the breach has occurred.

Activities that are 'likely to result in a high risk for the rights and freedoms of individuals', this can be a loss of financial data of personal data leading to potential fraud, or special data that has an impact on an individual's privacy

One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

The ICO has the power to compel us to inform affected individuals if they consider there is a high risk. In any event, the decision-making process must be documented as part of the investigation, in line with the requirements of the accountability principle within the GDPR.

Considerations, which may lead to a decision not to inform, include:

- Notification would result in undue stress, outweighing the benefit of notifying them.
- Are the individuals who would be notified capable of understanding the notification? For example, does the person have the capacity to understand? If not, you may need to notify a third party with the legal right to make

decisions on their behalf (e.g. a Power of Attorney). Consideration will also need to be given as to who needs to be notified when the individual concerned is a child.

- Are the numbers involved so large that notification would involve disproportionate effort? In order to establish if notification would involve disproportionate effort you would need to take into account the difficulties which would occur in the process of notifying against the potential benefit that the notification might bring to the individual.

As a general rule, it is recommended that the individual is advised unless you can clearly justify why it is not in the data subject's interest.

Individuals will not be notified in the following circumstances:

- Where Bury Council has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to people not authorised to access it) and that those measures were applied to the personal data affected by the personal data breach. An example of this would be that the data was encrypted.
- Where Bury Council has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.
- Where notification would require disproportionate effort. In such circumstances there would still be an expectation for there to be a public communication or similar measure to notify data subjects.

3. Information Governance investigation and evaluation – Stage 2

Once the Policy Compliance Team has received the completed incident report an assessment will be completed to review the incident, actions taken to mitigate any risks and advise on any further actions required.

The role of the Policy Compliance Team regarding information incidents is to:

- Review the incident and actions taken so far
- Consider if any further action is required

- Identify any requirements to avoid further breaches or similar incident occurring in the service area or corporately
- Agree an action plan with the investigating officer with relevant timescales
- Follow up on the actions to ensure they have been completed
- Escalate issues to the Data Protection Officer

When reviewing the breach, the Policy Compliance Team will also consider the technical and organisational measures that are in place to determine:

- If the incident occurred despite having the existing measures in place
- Had the policies and procedures been followed? If not, why not?
- Have the staff in the work area completed their Information Governance training? If not, why not?
- Are there any gaps in the process currently that allowed for the breach, what steps need to be taken to revise the process

The Policy and Compliance Team will also review:

- The likelihood of the incident reoccurring?
- Requirement for current policies and procedures be rewritten?

Consideration also needs to be given to whether or not the incident involved deliberate or reckless behaviour by an employee:

- For a deliberate act, disciplinary measures or prosecution should be considered, taking advice from Legal and HR
- For reckless behaviour, disciplinary measures and retraining, as appropriate should be considered, taking advice from HR.

Determine if the employee(s) concerned in the incident was aware of current policies and procedures.

- If yes, did they comply?
- If not, why not?

Finally, the Policy and Compliance Team will review the potential impact from the risk and conduct a risk analysis which will determine if the incident is reportable to the ICO.

At this stage the Policy and Compliance Team will discuss the incident with the Data Protection Officer and consider if there are any containment actions that will remove the need for notification to the ICO. Under the following circumstances notification may not be necessary:

- the data is protected by means of encryption
- the personal data is recovered from a trusted partner organisation; or
- where the council can null the effect of any personal data breach.
- where the risk analysis score requires the incident be reported to the ICO or the ICO and DHSC, the incident must also be reported to the DPO.

4. Data Protection Officer Referral – Stage 3

Once an information incident report has been referred to the DPO, the DPO will determine if the incident is to be reported to the ICO. The incident will also be reported to Bury Council Corporate Governance Group on a monthly basis, and taken for review at the Information Governance Incident Panel. A weekly discussion of any incidents will also be held with the SIRO to make them aware of the breaches and agree any action needed.

Corporate Governance Group;

The DPO will present all incidents to the Corporate Governance Group to provided strategic oversight. The Group will meet on a bi-monthly basis to consider any information incidents referred to it by the DPO and to review actions from previous breaches. The DPO will present their findings to the group.

The group consists of subject area experts throughout Bury Council whose areas will benefit from the learning as policies, systems and practice may require altering as a result of the occurrence.

Panel Members;	**Services Represented;**
Director of Law and Democratic Services & SIRO	Legal
Head of Governance	Council Data Protection Officer
Director of Finance	Finance

Assistant Director of DDAT	ICT
Director of Regeneration and Project Delivery	BGI
Director of Community Commissioning	Robert Arrowsmith
Assistant Director of Operations Strategy	Operations
Head of Fraud, Audit, Insurance & Risk	Fraud Audit, Insurance and Risk
Risk Manager	Risk

The responsibilities of the Corporate Governance Group will be to:

- Consider data breaches, security incidents and near misses and ensure lessons learnt are communicated to the organisation.
- Consider the Data Protection Officer's advice on whether data breaches meet the threshold for reporting to the Information Commissioner's Office
- Make recommendations to the organisation/ Service Area following a serious information incident.
- Monitor and track that recommendations are being implemented
- Monitor longer-term incident trends and patterns, to allow the organisation to reduce the number and frequency, and proactively mitigate against the impact of such incidents in future.
- Advise service areas of the outcome of breach investigations and assist them with implementing mitigating actions and to embed organisational learning.

- Agree any required action plans, appropriate responsible officers and relevant timescales for implementation
- Provide assurance to the Executive Management Team that learning is proactively being identified and the organisation is building this learning into the day to day operation and delivery of key programmes.

5. ICO Notification

ICO Notification will be determined by the DPO in liaison with the SIRO and where an incident is deemed to be notifiable this must be done within 72 hours of Bury Council becoming aware, that on the balance of probability a breach has occurred.

At this stage, if appropriate, the Caldicott Guardian will also be made aware of the notification to the ICO.

Where the ICO is to be notified, the appropriate ICO documentation will be completed by the Data Protection Officer.

The ICO will respond to the breach notification and may conduct further investigations, which may result in adjustments to policies and/or procedures and possibly result in financial penalties being imposed on the Council or members of staff.

Any interactions with the ICO regarding Bury Council breaches will be managed by the Data Protection Officer and reported into the Corporate Governance Group.

6. Compliance and Monitoring

Legal and Professional Obligations

Bury Council will take actions to comply with the relevant legal and professional obligations.

Training

Bury Council will provide relevant training both online and face to face to ensure that staff understand the legislation and its application to their role.

All staff must complete mandatory data protection training every year and undertake any further training provided by Bury Council to enable them to perform their duties appropriately specifically those staff responding to complaints, Subject Access Requests and Freedom of Information requests.

Completion of training will be monitored by the Policy and Compliance Team and all employees must have regard to the Data Protection Legislation and this policy when collecting, accessing, using, disclosing or destroying personal information. Failure to do so may result in disciplinary action and legal prosecution.

If an employee is in any doubt about what constitutes or how to handle a data breach they should speak to their line manager or contact the Policy and Compliance Team by emailing IG@bury.gov.uk.

Policy Review

This policy will be reviewed regularly by the Policy and Compliance Team to ensure that it is updated in line with any change in legislation.

Bury Council will continue to review the effectiveness of this policy to ensure that it is achieving it intended purpose.

Any breaches of the principles in this policy must be reported to the Policy and Compliance Team immediately; ig@bury.gov.uk.

Where staff fail to follow and comply with this policy it may result in disciplinary action via the HR channels.

Appendix

Appendix 1 – Information Incident reporting form (Breach form)

Information Governance Incident Reporting form (Breach Form)

This form should be completed by the Line Manager of the individual who has performed the breach. Please refer to the Information Governance Incident Procedure when completing this form and your investigation.

If you require further advice in relation to this incident please contact the Policy and Compliance Team (Contact details at the end of the form)

Section 1: Who is reporting the breach?	
Name	
Email address	
When did you become aware of the data breach?	Date: Time:
How did you find out about the breach?	

Section 2: Who performed the breach	
Name	
Email address	
Date of breach	
Directorate	
Service Area	
Have they completed their GDPR training within the last year?	Yes / No

Section 3: Line Manager and Head of Service details	
Name of line manager (if not same person as section 1)	
Email address	

Name of Head of Service	
Email address	

Section4: What type of Incident was it? (tick all that apply)			
Data posted, sent by email or verbally disclosed to incorrect recipient		Corruption of data (stored or manipulated inappropriately)	
Data deleted or amended		Lack of appropriate checks before disclosure e.g. redaction/ID checks	
Lost information		System misuse leading to data disruption	
Access by unauthorised person(s)		Inappropriate data being held	
Disclosure due to system configuration error		Password sharing	
Cyber incident – hacking, disruption		Data not updated when informed of changes	
Data stored in an insecure location		Disclosed on Inter/Intranet/ SharePoint	
Misuse of Data - Subject contacted inappropriately, data used for a none notified purpose etc			
Other, give one line indication:			
Was the breach related to a cyber incident?			

Section 5: What has happened?

Describe what happened in as much details as possible (**do not include personal data or acronyms**) including:

- What happened
- What went wrong
- How it happened

Has this type of incident happened before? If yes, please give details

Section 6: What data was included in the breach? (Tick all that apply)			
Racial or ethnic origin		Political opinions	
Religious of philosophical beliefs		Trade union membership	
Sex life data		Sexual orientation data	
Gender reassignment data		Health data (including conditions/disabilities)	
Basic personal identifiers (e.g. name, contact details)		Identification data, e.g. usernames and passwords	
Economic and financial data, e.g. credit card numbers, bank details		Official documents e.g. driving licence, passport	
Location data		Genetic or biometric data	
Criminal convictions, offences		Other (please provide details)	

Section 7: Who has been affected: (tick all that apply)			
Employees		Users	
Subscribers		School or College Pupils / Students	
Customers or prospective customers		Patients	
Children		Vulnerable adults	
Other (please specify)			
How many individuals have been affected?			

Section 8: Potential consequences
What are the potential consequences of the breach? Please describe the possible impact on the individual(s), as a result of the breach.

Please state if there has been any actual harm to individual(s)			
What is the likelihood that individuals will experience significant consequences as a result of the breach? (please tick)			
Very likely		Likely	
Neutral – neither likely not unlikely		Unlikely	
Very unlikely		Not yet known	
Please give an explanation / justification for the likelihood chosen above			

Section 9: Measures in place
Describe the measures you currently have in place to prevent this type of breach occurring (e.g. staff training, documented processes/procedures, changes to system controls, access control etc.)
Describe the actions you have taken, or propose to take as a result of the breach (Include actions you have taken to fix the problem, and to mitigate any adverse effects e.g. confirmed data sent in error has been destroyed, updated passwords, additional training.)
Any other actions taken? (e.g. where the incident involves the loss of IT equipment have IT been informed?)
If there is any further information that you think we should know, please enter it here:

Office action only:		
	Yes	**No**
Has the data breach been logged?		
Has a letter been sent to the member of staff		
Does the data breach need reporting to the ICO?		
Date discussed with DPO:		
DPO recommendation		
Date reported to ICO		
Next steps:		