RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

PROCEDURE FOR INVESTIGATING INFORMATION SECURITY INCIDENTS & EVENTS

Version: FINAL v.1.5 wef 22.10.2025

Content

Appendix

Introduction

In keeping with the Council's Information Security Policy, a consistent and robust approach to investigating information security incidents and events must be maintained across the Council. All incidents and events must be handled and investigated appropriately to establish the facts, identify corrective and preventative actions, and ensure ongoing protection of Council data, systems, and assets.

This procedure sets out the steps to be followed when **investigating** any information security incident or event, and applies to all employees, elected members, contractors, third-party suppliers, and anyone with access to Council data, systems, or assets.

Related Documents:

This procedure should be read in conjunction with the Council's **Procedure for Reporting Information Security Incidents & Events**, which outlines how incidents and events should be reported. Both documents, along with the Information Security Policy, can be found on RCT Source or Inform (*Support Services* > *Information Management* > *Policies)*.

Note for Elected Members:

Elected Members should refer to the **Elected Member ICT, Internet & Email Acceptable Use Policy** and the Members Portal for access to relevant documentation and guidance on their specific responsibilities.

1. Initial Review of Security Call

When an information security call is raised by the ICT Service Desk, it will be routed to the Information Management Team and/or Cyber Security Team for initial review, depending on the nature of the issue.

The first step is to assess the nature of the security concern (e.g., cyber-related, personal data breach etc.). If personal data is involved, it is important to determine whether a personal data breach has occurred. A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes both accidental and deliberate incidents and is not limited to the loss of personal data.

Following this assessment, the call will be classified as either an **event** or an **incident**:

- **Events**

  Events are typically potential or internal breaches of security. Examples include:
  - Internal communication errors (e.g., email sent to the wrong department or officer)
  - Loss of an encrypted device containing personal data (e.g., mobile phone, laptop, tablet)

- **Incidents**

  Incidents are more serious and have, or are likely to, result in a security breach that may compromise the confidentiality, integrity, or availability of Council data, systems, or assets. Examples include:
  - External communication errors (e.g., letter or email sent to the wrong recipient containing personal information)
  - Inappropriate disclosure of personal information (e.g., verbally or erroneous posting of information on the Council website)
  - Loss of a hard copy paper file containing personal information
  - Malware (e.g., virus) that has penetrated the Council’s network

Determining if the call is an incident or event

To decide whether a call should be treated as an event or an incident, the Information Management Team, the Cyber Security Team, or both (depending on the nature of the breach), will consider factors such as:

- Whether a breach has occurred, or whether there is potential for a breach if preventative measures are not taken
- The sensitivity of the information affected
- The number of data subjects affected
- The potential impact on the data subjects (e.g., risk to their rights and freedoms)
- The potential impact on the Council
- Actions taken to contain or recover from the situation
- Whether the data was encrypted (in cases of loss or theft)
- Whether the disclosure was internal (between Council employees) or external (e.g., member of the public)

If there is uncertainty about how to classify the call, the matter will be referred to the Information Security Group for a decision.

2. Dealing with an Information Security Event

Information security events will be referred to, and dealt with by, the Information Management Team and/or Cyber Security Team, working directly with the relevant service manager. For events involving Elected Members, the Monitoring Officer will act as the point of contact.

Events are formally recorded but are typically managed through informal advice and guidance rather than a full incident investigation. No incident report is required for events. The Information Management Team and/or Cyber Security Team will provide advice to the manager (or Monitoring Officer, for Elected Members) on appropriate actions to address the event, and the manager is responsible for implementing any recommended actions.

3. Dealing with an Information Security Cyber Incident

Cyber incidents with be dealt with in accordance with the following procedures:

- Cyber Incident Response Plan
- ICT Procedure for dealing with a Phishing Incident or Event

4. Dealing with an Information Security Incident

All incidents will be fully investigated to establish the facts and identify any corrective and/or preventative actions required. Not all incidents will require the same depth of investigation; the approach will be proportionate to the circumstances and severity. The purpose of the incident investigation is to:

- Establish the facts and determining what went wrong - extent of the breach, amount and sensitivity of information involved
- Identify the severity and potential impact of the incident on the Council and on individuals affected (including assessing whether there is a high risk to their rights and freedoms, and whether they need to be informed of the incident).
- Identify any potential for loss or damage to the Council or any other body
- Identify risks that are appropriate for follow up and action
- Make recommendations to address identified risks
- Inform future business processes and planning
- Determine whether to report the incident to the Information Commissioner (if it involves personal data) and or any other regulatory body

The incident investigation process will be led by the Information Management Team and/or the Cyber Security Team, in conjunction with the relevant Head of Service. Depending on the nature and severity of the incident the investigation may involve:

- Collecting and recording of evidence
- Meeting with those involved
- Taking statements, formal or informal, from those involved including any witnesses
- Consulting or engaging the Council's Human Resources, Internal Audit and/or Legal Services departments
- Reporting the incident to the Information Commissioner's Office where a serious breach has been identified that impacts on the rights and freedoms of the affected
- Informing the individual affected (data subjects) where it has been identified that there may be a high risk to their rights and freedoms.
- Involving the Council’s Press Team where the incident has or is likely to be made public.

5. Incidents Involving Personal Data

Where personal data is affected by an incident, the Information Management team will carry out an assessment to determine whether it meets the GDPR definition of a personal data breach.

Risk Assessing a Personal Data Breach

If an incident is assessed as a personal data breach, a risk assessment will be undertaken by the Data Protection Officer (or delegated officer) in consultation with the relevant Head of Service, to determine the actual or potential impact on the rights and freedoms of affected individuals. This **must** be done within **72 hours** of becoming aware of the breach, to comply with the Information Commissioners Office reporting requirements.

In risk assessing the personal data breach the Data Protection Officer and Head of Service will consider:

- The nature of the breach
- The number of data subjects affected
- The categories of data subject affected
- The volume of data affected
- The categories of data affected and their sensitivity
- How easily individuals can be identified
- Measures taken to contain the incident
- Potential or actual consequences / adverse effects on the individuals affected by the incident, including:
    - Privacy
    - Personal financial interest
    - Other material damages
    - Health and safety
    - Emotional wellbeing
    - Other non-material damages.

Reporting the Personal Data Breach to the Information Commissioners Office

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Data Protection Officer will refer the breach to the Senior Information Risk Owner or a delegated officer, along with their advice and recommendations. The Senior Information Risk Owner (or delegated officer) is responsible for considering the circumstances and the advice provided by the Data Protection Officer, and for making the decision as to whether the breach should be reported to the Information Commissioners Office. The Data Protection Officer must not report the breach to the Information Commissioners Office unless and until explicit instruction to do so has been given by the Senior Information Risk Owner or delegated officer.

When reporting a breach to the Information Commissioners Office the Data Protection Officer will use the Information Commissioners Office reporting form and provide:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Officer or another contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to address the personal data breach and, where appropriate, the steps taken to mitigate any possible adverse effects

Breaches that require reporting to the Information Commissioners Office must be reported within 72 hours of the Council becoming aware of the breach, unless there is a clear and justifiable reason for delay. Any delay beyond 72 hours must be accompanied by an explanation for the late reporting.

Notifying data subjects of a personal data breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will inform those affected directly and without undue delay.

Responsibility for notifying individuals rests with the relevant Service, who must do so in consultation with the Information Management Team. The Information Management Team will provide expert advice and support to ensure that notifications are accurate, timely, and compliant with legal requirements.

No notification to data subjects should be made unless and until the approach has been agreed with the Information Management Team.

6. Actions and Recommendations Identified During an Investigation

Following the conclusion of an incident investigation, actions and recommendations will be identified to mitigate, as far as possible, the risk of a similar incident occurring in the future. All actions and recommendations must be recorded in the incident investigation report.

Each action will be assigned a due date for completion and allocated to a responsible officer. The responsible officer must confirm, by signing the report, their commitment to complete the actions within the specified timeframe. It is the responsibility of the assigned officer to ensure that all actions are completed in accordance with the investigation report and by the agreed due date.

Actions will be monitored by the Information Management Team and/or the Cyber Security Team, depending on the nature of the breach. If actions are not completed within the agreed timeframe, the matter may be escalated to the Information Management Board and/or the relevant Head of Service or Service Director for review and further action.

Appendix I: Quick Reference Workflow: Investigating Information Security Incidents & Events

1. **Security Call Raised**
    - ICT Service Desk logs the call and routes it to Information Management Team and/or Cyber Security Team.

2. **Initial Assessment**
    - Information Management Team and/or Cyber Security Team assess the nature of the issue (e.g., cyber-related, personal data breach).
    - If personal data is involved, Information Management Team and/or Cyber Security Team consider if a personal data breach has occurred.

3. **Classification**
    - Information Management Team and/or Cyber Security Team classify the call as either an event (potential/internal breach) or an incident (actual/likely breach with impact).
    - If uncertain, Information Management Team and/or Cyber Security Team consult the Information Security Group.

4. **Event Handling**
    - Information Management Team and/or Cyber Security Team manage the event with relevant manager.
    - Provide advice/guidance; no formal incident report required.
    - Manager implements recommended actions.
    -

5. **Incident Handling**
    - Information Management Team and/or Cyber Security Team lead the investigation with the relevant Head of Service.
    - Collect evidence, interview involved parties, consult HR/Legal as needed.
    - Assess impact, identify corrective/preventative actions.

6. **Personal Data Breach (if applicable)**
    - Data Protection Officer (or delegate) conducts risk assessment within 72 hours.
    - Data Protection Officer refers to Senior Information Risk Owner or delegated officer for decision on ICO reporting.
    - Data Protection Officer only reports to ICO if instructed by Senior Information Risk Owner or delegated officer.
    - Service notifies affected individuals in consultation with Information Management Team.

7. **Actions & Monitoring**
    - Information Management Team and/or Cyber Security Team record actions/recommendations, assign responsible officer and due date.
    - Action owners (responsible officers) complete assigned actions within the agreed timeframe.

- Information Management Team and/or Cyber Security Team monitor completion; escalate incomplete actions to Information Management Board and/or relevant Head of Service/Service Director.

Version Control

Version No	Date approved by Information Management & Cyber Security Team	Valid from	Valid to	Changes Made
1.0	10.08.2016	10.08.2016	10.08.2017	New procedure developed based on former Information Incident Investigation policy.
1.1	11.08.2017	11.08.2017	01.10.2019	Reviewed by IM team – no changes
1.2	02.10.2019	02.10.2019	27.11.2022	Amended ICO reporting requirements, job titles and timescales/process for incidents/events to reflect current working practices.
1.3	28.11.2022	28.11.2022	12.11.2024	Reviewed. Section numbering and Contents page updated.
1.4	13.11.2024	13.11.2024	21.10.2025	
1.5	22.10.2025	22.10.2025		General review and update. Added reference to Cyber Security Team. Incident/event decision – changed to consult with Security Group for decision rather than DPO Events - removed reference to IM champion – replaced with HoS. Visio document replaced with quick reference workflow.