RHONDDA CYNON TAF

RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

PROCEDURE FOR REPORTING INFORMATION SECURITY INCIDENTS & EVENTS

Version: FINAL v2.3 wef 22.10.2025

Content

Appendix

Introduction

In keeping with the Council's Information Security Policy, employees, elected members, contractors, third-party suppliers, and anyone with access to Council data regardless of format, systems, or assets, have a **personal responsibility** to **report** any potential, suspected, or actual information security incident or event as soon as they become aware of it.

This procedure sets out the steps to be followed when **reporting** 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 Investigating Information Security Incidents & Events**, which outlines how incidents and events should be investigated. 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. Why do I have to report an information security incident / event?

Reporting information security incidents or events is essential to maintaining a safe and secure working environment across the Council. It safeguards the **confidentiality, integrity, and availability** of our data, systems, and assets, and plays a critical role in effective risk management.

Timely and accurate reporting enables the Council to:

- **Respond quickly** to contain and mitigate potential harm
- **Identify patterns and vulnerabilities** through trend analysis
- **Strengthen preventative measures** and improve staff awareness
- **Protect public trust** by demonstrating accountability and transparency

1.1 Information security incidents / events relating to personal data

When processing personal data, the Council has a legal obligation to comply with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). These regulations require organisations to have robust incident management procedures in place to detect, report, investigate, mitigate, resolve, and learn from any information security incident or event involving personal data (referred to as a *personal data breach*).

If a personal data breach is likely to pose a risk to the rights and freedoms of individuals affected, the Council must notify the Information Commissioner's Office (ICO) within **72 hours** of becoming aware of the breach. If the breach is likely to result in a **high risk** to individuals' rights and freedoms, the Council must also notify those affected individuals **without undue delay.** Failure to notify the ICO or affected individuals when required may result in enforcement action. It is therefore imperative that **any** information security incident or event, no matter how minor it may seem, is reported immediately and in accordance with this procedure.

Note: The Council is required to keep a record of **all** personal data breaches, regardless of whether the ICO and/or individuals are notified.

2. What is an information security incident / event?

The term ***information security incident/event*** is broad and can cover a wide range of situations. While it's not possible to list every potential scenario, it generally refers to any actual, suspected, or potential breach of security that may compromise the **confidentiality, integrity, or availability** of Council data, systems, or assets.

Incidents and events may include, but are not limited to:

- **Loss or theft** of personal, confidential or commercially sensitive information in paper form.
- **Loss or theft** of a Council device - such as a PC, laptop, tablet or phone (even if the device is encrypted).
- **Communication errors** e.g. emailing personal, confidential or commercially sensitive information to the wrong person, sending a letter to the wrong address etc.
- **Accidental disclosure** of personal, confidential, or commercially sensitive information
- **Unauthorised access** to Council systems or data, e.g. an employee accessing data for personal reasons
- **Malicious or inappropriate destruction, modification or alteration** of Council data systems, systems or assets regardless or format (physical or electronic).
- **Unauthorised access** to data by a third party
- **Computer virus or malware**
- **Receiving phishing emails**
- **Sharing passwords** with unauthorised individuals

Examples of the most common types of information security incidents and events can be found in **Appendix I**. This list is not exhaustive.

Note: All staff must report any issue where they have a **reasonable belief** that there is a risk to the security of personal, confidential, or commercially sensitive data, **no matter how minor it may seem**.

3. How to report an information security incident / event

Employees

Employees, agency staff, trainees, individuals on work placements, and anyone working for or on behalf of the Council (whether temporary or permanent) must report any potential, suspected, or actual information security incident or event immediately to:

- Their Line Manager, and
- The ICT Service Desk

Elected Members

Elected Members must report any potential, suspected or actual information security incident or event immediately to the Council's Monitoring Officer, who will then notify the ICT Service Desk on their behalf.

Contractors, third party suppliers

Contractors, third-party suppliers and anyone with access to Council data, systems, or assets must report any potential, suspected, or actual information security incident or event immediately to the designated Council contact, as defined in the relevant contract, data access agreement, or other governing documentation.

It is recommended that information security incidents or events are reported to your Line Manager (or the Monitoring Officer) and the ICT Service Desk by telephone on 01443 570000, wherever possible.

Reporting by phone helps ensure that an ICT Security call is promptly raised and routed to the appropriate team for action.

4. What information is required when reporting?

It’s important to provide as much detail as possible when reporting an information security incident or event. This enables the Information Management / Cyber Security team to quickly assess the nature and severity of the situation, evaluate the potential level of risk and impact, and take appropriate containment measures.

While the specific details may vary depending on the type of incident or event, the following information should be provided **at a minimum**:

- ✓ Name, directorate/department, job title and contact details of person reporting the incident.
- ✓ Name, directorate/department, job title and contact details of person responsible for incident (where known or where applicable).
- ✓ Description of the potential, suspected or actual incident or event.
- ✓ Date and time the incident or event occurred.
- ✓ Location of incident or event (if applicable)
- ✓ The categories of data affected by the incident or event (e.g. financial information, health information) (Note: Do not include or share any actual personal data, copies, or extracts when reporting to the ICT Service Desk. Only the category is required at this stage. If further detail is needed for the investigation, it will be requested later).
- ✓ Where personal data is affected, provide the approximate number of individuals and the types of individuals to which the data relates (e.g., service users, employees, customers).
- ✓ The type, asset numbers and location of equipment affected (where applicable).
- ✓ Whether the security incident / event puts any person or other data at risk.
- ✓ Any action already taken to recover/contain the situation.

Providing clear and complete information helps ensure a swift and effective response. If you're unsure whether something is relevant, it's better to include it than leave it out.

Please note: depending on the nature of the incident or event, further detailed information may be required during the investigation process.

5. What happens next?

Once an information security call is logged, the ICT Service Desk will assign it to the appropriate team, such as the Information Management Team, the Cyber Security Team, or both, depending on the nature and complexity of the incident.

The assigned team will carry out an initial review of the call. If needed, the person who submitted the call may be contacted to:

- Provide additional information
- Assist with immediate containment actions

Following this, the incident or event will be investigated in accordance with the Council's **Procedure for Investigating Information Security Incidents & Events.**

6. Key points to remember

- **Always report incidents or events**, even if you believe no harm has occurred
- **Report promptly and without delay** - timely reporting helps protect Council data, systems, and assets
- The incident procedure applies to **all types of data, systems and assets** – not just personal data
- The incident process is designed to **fix issues and support learning**, not to assign blame
- If you're unsure what to report or need further guidance, contact the ICT Service Desk, Information Management or Cyber Security team.

Appendix 1: Examples of Information Security Incidents and Events

Below are examples of common information security incidents and events. This list is **not exhaustive** but is intended to illustrate the types of issues that should be reported as potential, suspected, or actual information security breaches.

ICT Access Controls

- Sharing passwords with others
- Using another user's credentials (username and password)
- Writing down passwords and leaving them visible or accessible to others

ICT Security

- Receiving phishing emails requesting personal, sensitive, or confidential information
- Receiving unsolicited emails of an offensive nature
- Forwarding chain emails that encourage mass distribution
- Antivirus warnings appearing on your device
- Use of unapproved or unlicensed software
- Detection of malware, ransomware, or other malicious software

ICT Devices

- Loss or theft of portable media (e.g. DVDs, USBs, memory cards), even if encrypted
- Loss or theft of Council hardware (e.g. PCs, laptops, tablets, phones, printers, cameras), regardless of stored data
- Devices that cannot be located or accounted for (e.g. missing from expected storage locations)

Data Transfer (Fax, email, post, etc)

- Sending personal, sensitive, or confidential information to the wrong recipient
- Sending incorrect or excessive personal, sensitive or confidential information
- Including irrelevant personal data in communications by mistake

Inappropriate Disclosure

- Unknown individuals requesting access to Council data, systems, or assets
- Disclosing personal, sensitive or confidential information to someone without proper authorisation - verbally, in writing, or electronically
- Accidentally or intentionally publishing sensitive information online
- Inaccurate or inappropriate information published on the Council's website
- Unauthorised disclosure of information to the press or media

Data Loss

- Loss of personal, sensitive or confidential information in transit, regardless of format
- Information that can no longer be located or accounted for
- Uncollected printouts containing sensitive data left on printers or multi-function devices
- Letters or documents that fail to reach their intended destination

Disposal of Information

- Failing to securely dispose of paper-based sensitive information (e.g. not shredding)
- Storing sensitive information insecurely while awaiting disposal
- Failing to dispose of ICT devices securely via the ICT Service Desk

Physical Security

- Loss or theft of information in any format (e.g. hard copy files, computer equipment)
- Storing sensitive information in unsecured locations (e.g. unlocked cupboards, rooms, public areas)
- Unsecured areas where sensitive information is held

Unauthorised Access/Disclosure

- Accessing or disclosing personal, sensitive or confidential information without proper authorisation or consent.
- Sharing personal, sensitive or confidential information with unauthorised individuals
- Selling or offering to sell unlawfully obtained personal, sensitive or confidential information

Version Control

Version No	Date approved	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	10.08.2017	11.08.2017	24.05.2018	Reviewed by IM team – no amendments
2.0	19.03.2018	25.05.2018	27.11.2022	Reviewed in line with GDPR requirements.
2.1	28.11.2022	28.11.2022	12.11.2024	Routine review by DPO. No significant changes apart from format.
2.2	13.11.2024	13.11.2024	21.10.2025	Reviewed due to changes in ICT Service Desk call reporting process.
2.3	22.10.2025	22.10.2025		Changes following feedback from Elected Members - update to make clear reference to supporting procedure for **investigating** incidents and events. Also, general review of wording, grammar etc.