CITY OF
WOLVERHAMPTON
COUNCIL

# Information Incident Management Policy

**Change History**

| Version | Date | Description |
|---|---|---|
| 0.1 | 04/01/2013 | Draft |
| 0.2 | 26/02/2013 | Replaced procedure details with broad principles |
| 0.3 | 27/03/2013 | Revised following audit review |
| 0.4 | 26/04/2013 | Revised following IGB consultation |
| 2.0 | 14/06/2018 | Revised taking account of GDPR and Data Protection Act 2018 |

# Contents

## 1. Purpose

Information incidents giving rise to threats to the confidentiality, integrity and availability of the Council's information are increasingly a part of everyday business. The Council through its information governance and security policies seeks to minimise the frequency of such incidents.

The aim of this policy is to ensure that the Council reacts appropriately to any actual, or suspected, information incidents relating to any of its information, be it digital, paper-based or any other media.

This Information Incident Management policy is a key element in ensuring that the Council:

- Understands and recognises actual or suspected information events and incidents when they arise.
- Acts in a way that ensures that the event or incident is managed and resolved promptly, minimising the impact upon the public, service users, the Council and its employees.
- Investigates incidents promptly, properly and learns any lessons necessary to ensure a cycle of continual improvement of information security.

The aim of this policy is to ensure that the Council achieves the above by requiring:

- A single information incident contact and logging point.
- A documented set of management procedures that provides a consistent approach to ensure compliance with GDPR / Data Protection Act 2018 requirements.
- Prompt evaluation, escalation and remedial action
- An investigation and reporting procedure
- Risk management procedures to be applied

## 2. Scope

This policy applies to all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who use the Council's information, ICT facilities and equipment, or have access to, or custody of, customer information or WCC information.

All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the Council's information assets.

All users have a role to play and a contribution to make to identifying potential risks to the safe and secure use of information and any Information technology.

## 3. Definition

Under the General Data Protection Regulations (GDPR) a personal data breach is defined in Article 4(12) and in the Data Protection Act 2018 Chapter 1 paragraph 33 (3) as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

A personal data breach could lead to a loss of control over data, limitation of rights, reputational damage and other social or economic disadvantages.

Incident management is concerned with intrusion, theft, the compromise and misuse of information and information resources, and the continuity of critical information processes.

Examples of Information Incidents are given in Appendix 1.

## 4. Policy

### 4.1 Incident Management Principles

This policy sets out the principles for the management of information incidents below.

The principles are:

- A single information incident contact point for all types of information incident (manual, electronic, etc).
- Information capture / logging of all information events confirmed as incidents.
- Guidance available for information users on reporting information events and incidents.
- Progress/tracking information logged from initial assessment through to incident resolution.
- Identified time critical tasks with set targets and escalation steps.
- Assessment of potential severity / risks to the rights and freedoms of individuals as early as possible, to determine the appropriate incident management actions.
- Standard assessment of incident severity consistent with risk management guidance.
- High severity or potential high severity incidents or to be referred to the Senior Information Risk Owner as soon as identified.
- Procedures to allocate an investigation to an appropriate investigation officer according to the type of incident.
- Specific procedures to cover incident issues such as communications protocols and preservation and collection of evidence.

- Severe incidents will be reported in a Post Incident Review to Information Governance Board. The Corporate Risk Register to include all identified risks arising from such incidents.
- Summary reports of non-severe incidents to Information Governance Board.
- All procedures maintained and reviewed annually or as required.

Though all information incidents will be reported to a single contact point, distinction is drawn from that point between ICT technical incidents (e.g. malware, software malfunction, hacking incidents) and those involving disclosure of electronic/manual records or end user behavior, which will necessarily follow different investigation and incident management routes, but should still comply with the above principles.

## 4.2 Responsibilities

### 4.2.1 All Information Users

It is the responsibility of all Council information users to be able to identify potential information events/incidents and weaknesses and to take immediate action to report these directly to the Information Incident Contact Point or their line manager once identified.

### 4.2.2 Managers

All managers should ensure that their employees are aware of their obligations under this policy and support them in meeting these obligations.

### 4.2.3 Service Providers and Partnership Working

Any information event/incident that involves Council information must be reported without delay. This should be a contractual requirement where a service contract exists and included in any information sharing agreement for the sharing of personal information. Council managers and employees must be aware of similar obligations to other agencies if a data breach involves their information.

### 4.2.4 Information Incident Contact Point

The contact point procedures must ensure that all events/incidents that are reported are promptly recorded and forwarded to the appropriate managers/employees for action.

### 4.2.5 Information Governance Board

The Information Governance are responsible for implementing and monitoring compliance with this policy.

### 4.2.6 Chief Cyber Officer / ICT Security

ICT security are responsible for documenting, maintaining and implementing the wide range of technical standards required to safeguard the Council’s information. The Chief Cyber Officer is responsible for overseeing the arrangements to ensure the IT network security risks are properly considered.

### 4.2.7 Senior Information Risk Owner (SIRO) / Information Asset Owners

The SIRO is responsible for ensuring that the obligations of the Data Controller relating to personal data breaches are met. This is achieved by appropriate incident management plans being put in place as soon as possible to deal with high risk incidents. The SIRO is also responsible, with support from Information Asset Owners[1], for ensuring that all incidents are subject to investigation and subject to information risk management processes.

### 4.2.8 Caldicott Guardian

The Caldicott Guardian will be involved in the incident management process where the information incident involves Adult, Children’s or Public Health information, to fulfil their role of championing the fair, legal and ethical treatment of service user information within social care.

### 4.2.9 Data Protection Officer

The Data Protection Officer will be advised of all information incidents affecting personal information and will advise on related obligations in relation to personal data breaches and act as the contact point with the Information Commissioner’s Office in liaison with the SIRO.

### 4.2.10 Audit Services

Audit Services are responsible for reviewing incident procedures and plans, providing advice where securing evidence is an issue and or the involvement of the Police is possible, undertaking investigations, undertaking reviews and providing advice as required under this policy.

## 4.3 Compliance

Compliance with this policy will be monitored and reviewed by the Data Protection Officer who will report to the SIRO/Information Governance Board.

## 4.4 Review

This policy will be reviewed at least annually or when required by changed circumstances.

---

[1] Information Asset Owners have designated responsibility for specific Information governance and security arrangements relating to their Information Asset

## Appendix 1 – Examples of Information Events and Incidents

Examples of the most common Information Security Events and Incidents are listed below. It should be noted that this list is not exhaustive.

- Criminal events:
  - Theft of equipment, data or information, fraud or fraudulent activities;
  - ‘Blagging’ offences where information is obtained by deception e.g. unknown people asking for information, such as a password or details of a third party, that could gain them access to Council data or receiving unsolicited mail that requires you to enter password data;
  - Attempts (either failed or successful) to gain unauthorised access to data or information stored on computer systems e.g. hacking;
  - Copyright issues;

- Technical events:
  - Changes to information or data or system hardware, firmware, or software characteristics without the Council’s knowledge, instruction, or consent e.g. malware (viruses, Trojans etc.); use of unapproved or unlicensed software on Council equipment;
  - Unwanted disruption or denial of service to a system e.g. spam attacks; receiving unsolicited mail of an offensive nature; receiving and forwarding chain letters – including virus warnings, scam warnings and other emails that encourage the recipient to forward onto others;
  - Hardware/software failures;

- People Events:
  - Accidental loss of equipment, data or information including handheld devices such as Blackberries;
  - Failing to lock a PC screen when left unattended.
  - Human error e.g. emailing personal and/or sensitive personal information outside of the Council’s network either in error or without appropriate security measures in place;
  - Sharing/transfer of data or information, including personal and/or sensitive information with those who are not entitled to receive that information; without the consent of the data subject; and sharing more than the necessary amount of personal/sensitive information to complete required tasks;
  - The unauthorised use of a system for the processing or storage of data by any person;
  - Accessing computer systems/applications using someone else’s authorisation e.g. user id and password; sharing access tokens or logins; leaving your desk without logging off;
  - Disclosure of passwords/writing it down, and leaving it on display where it would be easy to find and used by unauthorised users;

  - Printing or copying confidential information and not storing it correctly or confidentially e.g. leaving documents on photocopiers;

- Physical and Environmental events:
  - Unforeseen circumstances e.g. fire or flood;
  - Unsecure premises;
  - Unlocked/unsecured workstations.