Information Incident Management Policy

Wiltshire Council
Where everybody matters

Document Control

Reference Number	Version 2.1	Status Published	Sponsor(s)/Author(s) Tim Way, Sarah Davis-Solan
Amendments	2.0 Regular review 2.1 Incident information and reporting steps changed to reflect elearning advice		
Document objectives: To establish management procedures so the council recognises information security incidents, responds effectively and implements lessons learned			
Intended Recipients: Wiltshire Council Officers			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators: ICO self-reporting, NHS SIRI reporting			
Training/Resource Implications:			
Ratifying Body and Date Ratified	Information Governance Programme Board September 2017		
Date of Issue	September 2017		
Review Date	September 2018		
Contact for Review	Information Governance		
SIRO signature			

Associated Documentation:

Policies:
Information Governance Policy

- Information security Policy
- Information Governance Policy
- Information Governance Management Framework
- Mobile Working Policy
- Information Asset Change Policy
- Information Incident Management Policy
- Records Management Policy
- Information Classification Scheme
- Network Security Policy
- System Level Security Policy

Legal framework:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000

Codes of Practice and Guidance:

- Information Commissioner. Data Protection Act breach reporting
- https://ico.org.uk/for-organisations/report-a-breach/
- HSCIC IG Toolkit Serious Incidents Requiring Investigation
- Payment Card Industry Data Security Standards PCI-DSS https://www.pcisecuritystandards.org/
- CESG Good Practise Guide 18 Forensic Readiness Planning
- 10 Steps to Cyber Security – Incident Monitoring

Contents

1 Purpose

The threat to the information assets of Wiltshire Council (the council) that can compromise the confidentiality, integrity and availability of the council's information are increasingly a part of everyday business.

The aim of this policy is to ensure that the council reacts appropriately to any actual or suspected information security incidents.

This policy is a crucial element in ensuring that we:

- Understand and recognise information security events and incidents when they arise;
- Act swiftly to ensure that the event or incident is managed and resolved, minimising the impact upon the public, the council and its employees, volunteers and partners;
- Investigate incidents properly and learns any lessons necessary to ensure a cycle of continual improvement of information security.

The council will achieve this by implementing:

- A single information incident logging point;
- A documented set of management procedures to plan for, identify, contain, assess and report information incidents;
- Prompt evaluation, escalation and remedial action including activation of the council's Integrated Emergency Management Plan if necessary;
- An investigation and reporting procedure;
- Integration with information risk management activities.

2 Scope

This policy applies to all employees of the council, elected representatives, other workers who may not be directly employed by the council (e.g. agency workers, contractors, self-employed consultants, authorised 3rd party suppliers and duly authorised visitors) who use council information, ICT facilities and equipment, or have access to, or custody of, customer information or council information.

All users must understand and adhere to 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 in identifying potential risks to the safe and secure use of information and any Information technology.

3 Information Incidents - Defined

An information incident is an event with the potential for unauthorised access to, or loss or theft of Wiltshire Council information, or of equipment used to access that information. Examples of activities which can lead to Information Incidents are given in the Appendix A.

Our incident management is about quickly identifying what information has been lost, and what impact that will have, so that we can contain, manage and recover from the incident.

4 Incident Management Principles

The principles for the management of information incidents are set out below:

- Guidance and mandatory education for information users, on identifying and reporting information events and incidents;
- Planning and preparation for likely scenarios based on risks and previous incidents;
- A single information incident contact point for all types of information incidents;
- Logging of all information incidents, noting key facts including date of incident, date of report, response time line.
- Alerting the IG team at an early stage in the incident lifecycle to ensure a proportionate and effective response;
- Monitoring of incident from initial contact through to incident resolution;
- Identified time critical tasks with targets and clear escalation steps;
- Assessment of potential severity as early as possible, to determine the appropriate incident management actions;
- Standard assessment of incident severity, consistent with risk management guidance. (Utilising Health & Social Care Information Centre SIRI guidance for incidents in Social Care);
- High severity or potential high severity incidents or to be referred to the Senior Information Risk Owner as soon as identified;
- Allocation of investigation to an appropriate investigation officer according to the type of incident;
- Specific procedures to cover incident issues such as communications protocols, notification of necessary external organisations and the preservation and collection of evidence;

- Severe incidents will be reported in a Post Incident Review to the appropriate Management Board;
- Summary reports of non-severe incidents to Risk Management Board;
- The Information Risk Register to include all identified risks arising from information incidents;
- 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 manual records or end user behaviour, which will necessarily follow different investigation and incident management routes, but should still comply with the above principles.

5 Responsibilities

We are legally obliged to notify the Information Commissioner's Office (ICO) of any serious data breach within 72 hours of the incident being discovered. It's important that you report all incidents - regardless of whether they result in actual data loss - straightaway so that The IG team can assess the severity and advise on next steps. Provide all the information asked for as quickly as you can, so that we can meet our legal obligations.

Even where no information has been shared or lost, reporting in this way helps the IG team to identify weaknesses in our security and gives us an opportunity to fix it.

5.1 All Information Users

Everyone working for or with the council has a personal responsibility to protect its information assets. This includes being alert to information security threats and reporting any information incidents.

It is the responsibility of all users of the council's information to be able to identify potential security events and weaknesses and to take immediate action to report these directly.

- Report the incident using the Incident form on The Wire.
- Tell your manager immediately so that they can inform your Information Asset Owner (IAO) straightaway. If your manager is not available, contact your IAO – this is usually your Head of Service.
- If you can't report online, call the ICT Service Desk on 01225 718718 to report the incident.

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

5.3 Service Providers and Partnership Working
Any information security incident that involves the council's 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 security breach involves their information.

5.4 Information Asset Owners
Information Asset Owners have designated responsibility for specific information governance and security arrangements relating to their Information Assets and a lead responsibility for resolving any incidents related to their assets.

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

5.6 ICT Security
The Head of ICT is responsible for ensuring ICT Security incident management procedures are documented and implemented.

5.7 Senior Information Risk Owner / Information Asset Owners
The SIRO is responsible for ensuring that appropriate incident management plans are put in place as soon as possible to deal with high impact incidents. The SIRO is also responsible, with support from Information Asset Owners, for ensuring that all incidents are subject to investigation and subject to information risk management processes.

5.8 Caldicott Guardians
The Caldicott Guardians will be involved in the incident management process where the information security incident involves Community, Adult or 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.

5.9 Data Protection Officer
The Data Protection Officer will be advised of all medium and high impact incidents affecting personal information and should advise on communication with the affected data subjects and the Information Commissioner's Office in liaison with the SIRO.

5.10 Information Governance (IG) Team
The IG team will respond to and escalate reported events and incidents, on a case by case basis will escalate each one accordingly.

The IG team are responsible for reviewing incident procedures and plans and the monitoring of incident investigations. IG will also ensure arrangements have been put in place to call in specialist advice where securing evidence may be an issue or the involvement of the Police is possible.

6 Compliance

Compliance with this policy will be monitored and reviewed by the Information Governance Assurance Steering Group.

7 Review

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

8 Appendix A – Examples of Information Security 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.

8.1 People Events:

- Accidental loss of equipment, data or information including mobile devices;
- Failing to lock a device 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;

8.2 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 or other sensitive data (phishing emails);
- Attempts (either failed or successful) to gain unauthorised access to data or information stored on computer systems e.g. hacking;
- Breach of copyright.

8.3 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.

8.4 Physical and Environmental events:

- Unforeseen circumstances e.g. fire or flood;
- Unsecure premises; Unlocked/unsecured workstations.
- Building access by those who have not been granted permission.