information management & security

Gloucestershire COUNTY COUNCIL

Information Security Incident Management Policy

1.0 Policy Statement

Gloucestershire County Council (the council) will react promptly to any actual or suspected incidents, breaches or concerns relating to information, ICT equipment or systems. Incidents or concerns relating to Information Security will be investigated in accordance with the requirements of the General Data Protection Regulation (GDPR), to ensure a timely response and minimise the risk to individuals, the council and the information it holds.

2.0 Risk management

This policy aims to ensure an appropriate incident management process is in place, which will help to mitigate the following risks;

- Harm to individuals
- Damage to the council's reputation,
- Potential legal action
- Fines against the council or individuals,
- Service disruption,
- Non-compliance with legislation, and/or
- Financial costs.

This policy and the Information Security policy also aims to ensure that;

- All Councillors, employees, partners, contractors and third parties are aware of the procedure for reporting information security incidents, and any observed or suspected incident, or information security concern (commonly referred to as a 'Breach').
- There is a timely response to all reported incidents or concerns in accordance with this policy and the Information Security policy.
- Following recovery from an information security incident, existing controls are examined to determine their adequacy, and corrective action is taken to minimise the risk of similar incidents occurring.
- Information security incidents are monitored and reported to Information Board on a 6 monthly basis.

3.0 Scope

This policy applies to all councillors, employees, partners, contractors and third parties. All users must comply with this policy at all times when accessing the council's information however accessed. Breach of this policy may be dealt with under the council's Disciplinary and Dismissals Procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

4.0 Definitions

An information security incident is any action that may compromise the confidentiality, integrity (i.e., accuracy or completeness), or availability of information. Such incidents include information stored and processed electronically and in other forms, such as on paper.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, corruption, unauthorised disclosure of, or access to, personal data; including breaches that are the result of both accidental and deliberate causes.

An incident can be defined as, but is not restricted to, the following:

- Unauthorised or inappropriate access or attempts to access or use, information or systems.
- Deliberate or accidental action (or inaction) outside the scope of action of the defined process by a data controller or processor.
- Transfer of personal and/or special category and/or commercially sensitive information to those who are not entitled to receive it.
- Loss or theft of personal and/or special category and/or commercially sensitive information or ICT equipment.
- Unauthorised changes to information, system hardware, or software.
- Loss of availability of personal data e.g., unplanned system outage resulting in no access to data.
- A malware infection or cyber-attack where data is made unavailable via encryption or ransomware.
- Non-compliance with information security policies.
- Accessing information without a justifiable business need e.g., the record of family members and/or friends.

5.0 Reporting an Information Security Incident or Concern

The council operates an open, honest, and immediate reporting system. All councillors, employees, partners, contractors, and third parties have a duty to report any observed or suspected information security incident(s) or concerns as soon as

they become aware of them. Reports must be made by contacting one or more of the following (depending on the nature of the incident):

- The Information Management Service at informationsecurity@gloucestershire.gov.uk;
- ICT related breaches e.g., lost or stolen equipment or compromised systems should be reported to ICT Service Desk via Service Now.

Reports must provide all relevant information, including:

- Contact name and number of person reporting the incident/concern (unless reporting anonymously);
- Team/service manager; Location, date, time and circumstances of the incident/concern;
- Whether the incident involves unauthorised access, use, or loss of information and if so its protective marking or sensitivity;
- Whether the incident puts any person or other information at risk;
- Asset ID (if applicable).If reporting an information security incident or concern to Information Management Service, information must be detailed on the Information Security Incident of Concern Initial Report.

The person reporting an information security incident or concern will receive confirmation that their report has been received and will be dealt with appropriately in accordance with this policy.

This policy is supported by the Incident Response and Escalation Procedure.

If you hear or see anything at work which concerns you, these incidents can be reported via the council's speak up if it's not right procedure.

6.0 Investigating an Information Security Incident or Concern

When an incident or concern is reported, the council will ensure that an initial impact assessment is undertaken where appropriate; this will determine the severity of the incident, the seniority of the manager assigned to lead/manage the investigation, and the timescales for escalation to senior leadership where appropriate. It is the responsibility of the assigned information security adviser to ensure each incident or concern is investigated in accordance with the Information Security – Incident Response and Escalation Procedure.
All the above processes will be recorded on a centralised system.

7.0 Policy Compliance

Security breaches that result from a deliberate or negligent disregard of any security policy requirements may, in the council's absolute discretion, result in disciplinary action being taken against that employee. If breaches arise from the deliberate or negligent disregard of the council's security policy requirements by a user who is not a direct employee of the council, the council shall take such punitive action against that user and/or their employer as the council deems appropriate.

The council may refer the matter of any breach of the council's security policy requirements to the police for investigation and (if appropriate) the instigation of criminal proceedings if in the reasonable opinion of the council such breach has or is likely to lead to the commissioning of a criminal offence.

If you don't understand the implications of this policy or how it applies to you please contact the following for advice:

- The Information Management Service at informationsecurity@gloucestershire.gov.uk

8.0 Document Control

8.1 Document information

Owner:	Rob Ayliffe, Director of Policy, Performance and Governance. (Senior Information Risk Owner)
Author:	IMS/ICT Policy Group
Reviewer:	IMS/ICT Policy Group
Board(s) consulted:	
Date created:	July 2010
Next review date:	August 2026
Approval:	Information Board, September 2019 (v2.0)
Date of approval:	
Scheme of Delegation ref:	
Version:	2.5
Classification:	UNCLASSIFIED

8.2 Version History

Version	Version date	Summary of Changes
1.4	September 2015	Links to procedures updated. Updated procedures in sections 5 and 7 to show new response times and roles of Information Governance & Assurance Manager and Information Governance Officer. Review period updated to every three years.
1.5	April 2016	Update links due to new staffnet pages. Also included new severity rating scale which was approved by Information Board in April 2016
1.6	May 2018	Update links due to new IMS staffnet pages.
2.0	September 2019	Full review of policy, update of generic content and hyperlinks
2.1	October 2021	Minor changes for accessibility purposes including change of policy owner.
2.2	January 2023	Accessibility review and updates to formatting. Broken links fixed.
2.3	August 2023	Scheduled policy review
2.4	June 2024	Broken links fixed following migration of StaffNet to SharePoint
2.5	August 2024	Additional rows inserted into Documentation information table.

8.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

8.4 Contact Us

Email: informationsecurity@gloucestershire.gov.uk
Phone: 01452 324000