information
management & security

Gloucestershire
COUNTY COUNCIL

Gloucestershire County Council
Information Security Incident Management Policy

1. 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. Information Security incidents or concerns 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. 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 and/or fines against the council or individuals,
- Service disruption,
- Non-compliance with legislation, and/or
- financial costs.

Furthermore, this policy and the Information Security policy also aims to ensure that;

- All Councillors, employees, partners, contractors and third party users are aware of the procedure for reporting information security incidents, and their responsibility to promptly report 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.
- That 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.
- There are mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified, monitored, and reported.

3. Scope

This policy applies to all councillors, employees, partners, contractors and agents of the Council who use or who have access to the Council's information, systems, ICT equipment or ICT facilities.

All such users are expected to comply with this policy at all times when using the council's information, systems, ICT equipment, or ICT facilities,.Whether accessed locally or remotely (e.g. via the council's Remote Access Gateway, or via any council owned device). 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. Definition of an Information Security Incident

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

A personal data breach is further defined as 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 information security incident includes, 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) by a data controller or processor. Transfer of personal and/or special category (sensitive) information to those who are not entitled to receive it.
- Loss or theft of personal and/or special category (sensitive) information or ICT equipment.
- Unauthorised changes to information, system hardware, or software. Loss of availability of personal data.
- A virus infection or cyber attack where data is made unavailable via encryption or ransomware.
- Non-compliance with information security policies

5. Reporting an Information Security Incident or Concern

The Council encourages an open, honest and immediate reporting system that is used to minimise impact, improve practice and reduce risk. All councillors, employees, partners, contractors and agents of the council have a duty to report any observed or suspected information security incident(s), or information security 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 Service Desk via Service Now.

Incidents can also be reported via the Council's confidential reporting procedure.

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).

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.

6. Logging an Information Security Incident or Concern

Details of all information security incidents/concerns will be logged centrally on the Council's Information Security Incident Management system.

7. Investigating an Information Security Incident or Concern

When an incident or concern is reported, Information Security will ensure that an initial impact assessment is undertaken; this will determine the severity of the incident and the seniority of the manager assigned to lead/manage the investigation. It is then the responsibility of the assigned investigating officer to ensure each information security incident/concern is investigated promptly and thoroughly in accordance with the Information Security – Incident Response and Escalation Procedure.

Each investigation and its results must be fully documented by the Investigating Officer and all related documentation retained and stored centrally for 6 years by the Information Management Service.

The Information Assurance Manager and Information Security team have joint responsibility for ensuring that all information security incidents are investigated, documented, and reported to the Information Board.

In instances where a more detailed investigation or internal review is required the relevant director will be contacted and asked to nominate an appropriate senior manager. If, for any reason, the senior manager is unable undertake the investigation/internal review they will be expected to appoint an alternative manager of equal seniority.

8. 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. In the event that 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 in its absolute discretion deems appropriate.

The Council may, in its absolute discretion 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

9. Review and Revision

This policy will be reviewed every 12 months.

Document Control

Author:	Julia Evans, ICT Infrastructure Manager Sue Blundell, Corporate Information Security Advisor
Owner:	Rob Ayliffe, Director of Policy, Performance and Governance. (Chief Information Officer and Senior Information Risk Owner)
Document Number:	v2.1

Revision date	**Summary of Changes**	**Changes marked**
Sept 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.	V1.4
April 2016	Update links due to new staffnet pages. Also included new severity rating scale which was approved by Information Board in April 2016	V1.5
May 2018	Update links due to new IMS staffnet pages.	V1.6
Sept 2019	Full review of policy, update of generic content and hyperlinks	v2.0
October 2021	Minor changes for accessibility purposes including change of policy owner.	v2.1

Document Approvals

Version	**Approved by**	**Date**
1.1	Directors' Board	Sept 2010
1.2	Information Board	Sept 2011
1.3	Information Board	Dec 2012
2.0	Information Board	Sept 2019
2.1	No approval required	N/A