Gloucestershire County Council
Information Security Incident Management Policy

1.0 Policy Statement

1.1 Gloucestershire County Council (the Council) will react promptly to any actual or suspected incidents or concerns relating to information or ICT systems within the custody of the Council. Information Security Incidents or concerns will be reported, recorded and investigated in accordance with this policy and supporting procedures to provide timely remediation and minimise the risk to the Council and the information it holds.

2.0 Scope

2.1 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, computer equipment or ICT facilities.

3.0 Definition of an Information Security Incident

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

3.2 An information security incident includes, but is not restricted to, the following:

- Unauthorised access to, or use of, information or electronic processing/storage systems
- Transfer of personal and/or sensitive information to those who are not entitled to receive it
- Loss or theft of personal and/or sensitive information or ICT equipment
- Attempts (either failed or successful) to gain unauthorised access to information or a computer system
- Unauthorised changes to information, system hardware, or software
- A virus infection (unexpected or unusual behaviour of the workstation could indicate a virus infection)
- Non-compliance with information security policies

4.0 Risks

4.1 Compromise of information confidentiality, integrity, or availability could result in: harm to individual(s), detrimental effect on service provision, reputational damage, legislative non-compliance, and/or financial costs.

4.2 This policy aims to mitigate these risks by ensuring:

- 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.
- Timely remediation of reported incidents or concerns in accordance with this policy and the supporting Information Security - Incident Response and Escalation Procedure.
- That following recovery from the 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.

5.0 Reporting an Information Security Incident Concern

5.1 The Council encourages an open, honest and immediate reporting system that is used to minimise impact, improve practice and reduce risk.

5.2 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. Reports must be made to one of the following:

- ICT Service Desk on 01452 42 5999;
- Information Management Service on 01452 32 4260 or informationsecurity@gloucestershire.gov.uk ;
- Council's confidential reporting procedure

5.3 Information security incidents/concerns must be reported within two working days of the breach occuring. Reports must provide all relevant information, for example:

- Contact name, number of person reporting the incident/concern (unless 10.3 applies);
- 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).

5.4 The person reporting an information security incident or concern will receive confirmation within 2 working days that their report has been received and will be dealt with appropriately in accordance with this policy.

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

6.0 Logging an Information Security Incident or Concern

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

7.0 Investigating an Information Security Incident or Concern

7.1 When an incident or concern is reported, Information Security and/or the ICT Service, will ensure that an initial impact assessment is undertaken; this will determine the seniority of the manager assigned to lead/manage the investigation.

7.2 It is the responsibility of the 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.

7.3 Each investigation and its results must be fully documented by the Investigating Officer and the documentation retained and stored centrally for 6 years by the Information Governance Officer.

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

8.0 Policy Compliance

8.1 If you don't understand the implications of this policy or how it applies to you please contact the following for advice:
Information Management Service on 01452 32 4260 or
informationsecurity@gloucestershire.gov.uk

8.2 Any user who is found to have breached this policy may be subject to the Council's disciplinary procedure.

9.0 Policy Review

9.1 The current version of this policy can be found at http://staffnet/19838 along with information that supports this policy.

9.2 This policy will be reviewed as it is deemed appropriate or at least every 3 years.

10.0 Key Messages

10.1 All information security incidents or concerns must be reported immediately

10.2 All reported information security incidents and/or concerns must be promptly and thoroughly investigated.

10.3 We can maintain your anonymity when reporting an incident if you wish.

10.4 If you are unsure of anything in this policy you should ask for advice from Information Management Service on 01452 32 4260 or informationsecurity@gloucestershire.gov.uk

Document Control

Author:	Julia Evans, ICT Infrastructure Manager Sue Blundell, Corporate Information Security Advisor
Owner:	Jane Burns – Director of Strategy & Challenge (Chief Information Officer and Senior Information Risk Owner)
Document Number:	v1.4

Revision History Date of next revision: September 2018

Revision date	**Summary of Changes**	**Changes marked**
Oct 2009	First draft	v0.1
Apr 2010	Including amendments	v0.2
June 2010	Including amendments from Audit and Legal	v0.3
July 2010	Incorporating amendments from Information Management Team	v1.0
Sept 2010	Incorporating amendments from Information Board	V1.1
Jan 2012	Align all Information Security Policy review dates to Nov 2012 as agreed by Information Board 26/9/2011	V1.2
November 2012	Delete para 1.2 (ownership is covered in the document control table). Minor amendments to examples of infosec incidents and add non-compliance with information security policies. Replace references to Head of ICT with Programme Director. Amendments to reflect new ICT Service arrangements. Amendment to reflect that Sharepoint central recording is now in place.	V1.3
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.	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

Consultation This document has been distributed to:

Name	**Title**	**Date of Issue**	**Version**
Julia Evans	ICT Infrastructure Manager	Oct 2009	v0.1
Jenny Grodzicka	Corporate Information and Compliance Manager	Apr 2010	v0.1
Andy Gilbert	ICT Technology Manager	Apr 2010	v0.2
Sue Blundell	Principal IT Auditor	Apr 2010	v0.2
Will Felgate	Senior Lawyer	Apr 2010	v0.2
Tina Fable	HR Advisor	Apr 2010	v0.2
Heather Forbes	Head of Information Management & Archives	May 2010	v0.3

Document Approvals

Version	**Approved by**	**Date**
V1.1	Directors' Board	15 September 2010
V1.2	Information Board	26/9/11

V1.3	Information Board	19/12/2012
V1.4	Jane Burns	28/09/15