Gloucestershire County Council
Information Security Policy

1 Policy Statement

Information is an important asset; Gloucestershire County Council (the council) is committed to preserving the confidentiality, integrity, and availability of its information assets:

- For sound decision making;
- To deliver quality services;
- To comply with the law;
- To meet the expectations of its customers;
- To protect its customers, staff, partners, and reputation as a professional and trustworthy organisation.

The purpose of this policy is to protect the council's information and that of its partners, managing information risk and reducing it to an acceptable level, whilst facilitating the reasonable use of information to support normal business activity.

2 Risk Management

This policy aims to ensure an appropriate 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.

Information risk will be managed in accordance with the Council's Risk Management Policy Statement and Strategy. The SIRO, DPO and Corporate Leadership Team (CLT) will have oversight of information risk and the information risk management processes.

The council has standards for handling personal and/or special category (sensitive) information . These are applied throughout the council based on the

confidentiality/sensitivity of the information in use. Ownership of critical information and systems will be assigned to individuals, whose responsibilities are clearly defined and communicated to them on an annual basis (Information Asset Owners).

3 Scope

This policy applies to all councillors, employees, partners, contractors and agents of the council (i.e. users) who use or have access to council information, ICT equipment or ICT facilities.

All such users are expected to comply with this policy at all times when using the council's information, 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.

The policy applies throughout the lifecycle of any information, from creation, storage, and use to disposal. It applies to all information including:

- Information stored electronically on databases or applications e.g. email;
- Information stored on computers, mobile devices, printers, or removable media such as hard disks, DVD/CD rom, memory sticks, tapes and other similar media;
- Information transmitted on networks;
- Information sent by fax or any other communications method;
- All paper records;
- Microfiche, visual and photographic materials including slides and CCTV;
- Spoken, including face-to-face, voicemail and recorded conversation.

4 Definition of Information Security

Information security means safeguarding information from unauthorised access or modification to ensure its:

- **Confidentiality** – ensuring that the information is accessible only to those authorised to have access;
- **Integrity** – safeguarding the accuracy and completeness of information by protecting against unauthorised modification;
- **Availability** – ensuring that authorised users have access to information and associated assets when required.

5 Roles and Responsibilities

The Council's Senior Information Risk Officer (SIRO) is responsible for safeguarding information by:

- Initiating and overseeing the development and maintenance of the Information Security Policy and supporting documentation;
- Taking ownership of the Council's Information Security Policy, Incident Management Policy, and information risk assessment process to support and inform the Council's Annual Governance Statement;
- Advocating information risk management at Board level, ensuring Board members are adequately briefed and kept up-to-date on information risk issues;
- Reviewing and challenging the Information Security Risk Register, risks, controls, further actions, and progress, ensuring that identified information security risks are managed and mitigation plans are robust;
- Ensuring that the council's approach to information security and information risk assessment is communicated to all councillors, employees, partners, contractors and agents;
- Ensuring that information security arrangements are regularly reviewed to ensure that they comply with this policy and other security policies and standards in place.

The Data Protection Officer (DPO) is responsible for safeguarding information by:

- Providing information and advice about obligations to comply with the GDPR and other data protection laws;
- Ensuring provisions and processes are in place to:
    - Monitor compliance with the GDPR and other data protection laws, and with data protection polices,
    - Ensure the management of internal data protection activities;
    - Raise awareness of data protection issues
    - Train staff;
    - Conduct internal audits;
    - Provide advice on, and to monitor, data protection impact assessments;
    - Ensure co-operation with the supervisory authority; and
    - To have a point of contact for individuals whose data is processed (employees, customers etc.).
- Being the first point of contact for supervisory authorities.

Directors and managers are responsible for safeguarding information by:

- Promoting information security to all employees, contractors, partners and agents within their service area;
- Ensuring that employees understand and adhere to the Information Security Policy and its associated policies and procedures;

- Ensuring that information security requirements are specified in partnership agreements and third party contracts;
- Assigning Information Asset Owners for all information in their area of responsibility (Directors);
- Ensuring that regular information risk assessments are undertaken, and controls proportionate to the risk are implemented to protect their information;
- Ensuring that information security communications are effectively cascaded to all staff, partners, contractors and agents;
- Ensuring that information security is an integral part of all service processes;
- Providing the Directors' Assurance Statement on Information Risk Governance to inform the Council's Annual Governance Statement (Directors);
- Ensuring effective business continuity and disaster recovery plans are in place.

Information Asset Owners (IAOs) are responsible for safeguarding information by:

- Understanding what information is held, added, removed, how information is moved, who has access and why;
- Understanding and addressing risks to information assets;
- Undertaking information risk assessments for critical information assets on a regular basis. Ensuring that threats and vulnerabilities are identified, risks are assessed and appropriate decisions made regarding the risks that are accepted, and those to be mitigated by control measures to reduce the risk to an acceptable level;
- Updating information asset registers;
- Undertaking monitoring to ensure that security controls continue to be effective;
- Managing the residual information risk;
- Ensuring that in respect of their information asset, policies and procedures are followed;
- Providing assurance on the security and use of their information assets to their Director to inform the Council's Annual Governance Statement.
- Completing annual refresher training
- Ensuring appropriate handover of the role takes place if/when ownership changes.

The Information Management Service is responsible for safeguarding information by:

- Providing information security advice and support to the SIRO, DPO, Directors, Managers, IAOs and staff;
- Developing and maintaining appropriate information security policies, procedures and guidelines to protect the council's information;
- Promoting information security awareness and structured information risk assessment;

- Providing advice and guidance to enable IAOs to identify and manage information risks;
- Providing information security training.

ICT are responsible for safeguarding information by:

- Providing information security advice and support to the SIRO, DPO, Directors, Managers, and IAOs;
- Developing and maintaining appropriate information security policies, procedures and guidelines to protect the council's information;
- Being responsible for achieving national standards (PSN, Cyber Essentials Plus) and administering appropriate technical security controls;
- Providing advice and guidance to enable IAOs to identify technical information security risks and appropriate technical security controls.

6 Legal and regulatory requirements

Users of the council's information assets will abide by UK and European legislation relevant to information security including:

- General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Copyright, Designs and Patents Act 1988
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Civil Contingencies Act 2004
- Freedom of Information Act 2000

and any specific information protection standards relevant to council business such as the Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/security_standards/.
This list is not exhaustive and may change over time. Users should seek guidance about the legal constraints of using information in their work, and the council will provide appropriate guidance and training to its staff.

7 Actions in the event of an Information Security Breach

All employees and anyone who delivers services on the council's behalf (contractors, partners, agents or other third parties with access to the council's information assets), has a responsibility for immediately reporting any suspected or observed security breach, to comply with the ICO's 72 hour reporting deadline. Further details are provided at Reporting/investigating a security breach - Staffnet.

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 this policy to the police for investigation. If appropriate the council may also instigate criminal proceedings, if it is reasonable that such breach has or is likely to lead to the commissioning of a criminal offence.

9 Information Security Policy Exceptions

Exceptions will be granted only where there is a clear business case to do so, and where there is evidence that a risk assessment has been undertaken and any additional risks introduced by the exception are mitigated to an acceptable level. The approval of the relevant Director is required, and where this impacts on technical controls the approval of the Director of Corporate Resources is required.

All records of exceptions should be directed to the Information Security Team at informationsecurity@gloucestershire.gov.uk who will maintain a record.

10 Other supporting Information Security Policies, Standards and Procedures

- Data Protection Policy
- Card Payment Policy
- Information Security Incident Management Policy
- Incident Response and Escalation Procedure
- Information/IT Access Policy
- Software Management Policy
- Freedom of Information Policy
- Testing with Personal Data Standard
- Scanning Policy

All other supporting policies, standards, and procedures can be found at http://www.gloucestershire.gov.uk/council-and-democracy/strategies-plans-policies/information-management-and-security-policies/.

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

11 Policy Review

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

Document Control

Author:	Kirsty Benzie, Assistant Head of IMS (Caldicott Angel) (based on original by Sue Blundell, Information Security Advisor)
Owner:	Rob Ayliffe, Director of Policy, Performance & Governance (Senior Information Risk Owner)
Document Number:	v4.3

Revision date	Summary of Changes	Changes marked
September 2015	Links to policies and list of supporting policies updated. Review period updated to every three years.	2.3
April 2016	Links to staffnet pages updated to take in to account new IMS pages	2.4
January 2018	Links to staffnet pages updated to take into account new IMS pages. Reference to decommissioned GCSx encryption removed	2.5
May 2018	Updated links to DPA 2018 and removed reference to DPA1998 Amended author to reflect current Assurance Team Manager, included DPO role	3.0
August 2019	Full review of policy, update of generic content and hyperlinks	4.0
January 2020	Added GCC Card Payment Policy link to section 10, amended policy review date in line with PCIDSS requirements	4.1
August 2020	Updated author and policy owner details, re-named CoMT to CLT	4.2
December 2020	Update policy owner details	4.3

Document Approvals

Version	Approved By	Date
Version 2.3	Jane Burns	September 2015
Version 2.4		April 2016
Version 2.5		January 2018
Version 3.0		May 2018
Version 4.0	Information Board	September 2019
Version 4.1		January 2020
Version 4.2		August 2020
Version 4.3	Information Board	December 2020