Gloucestershire County Council
Information Governance Framework Policy

1. Policy Statement

Gloucestershire County Council (the council) recognises that information is a valuable asset, and is vital for the delivery of quality services and the efficient management of resources. Information Governance provides a coordinated approach for getting the best value from information while minimising associated risks.

Information Governance consists of a framework of overarching roles and responsibilities, policies, standards, procedures and guidance that covers all information disciplines and all information created, received, managed, shared and disposed of by the council. This framework enables the council to embed cultural and systematic good practice, identify and manage information risks, and monitor compliance.

As part of the requirements of GDPR, the council has reviewed how it demonstrates accountability for its processing activities.

The council is a public authority and therefore has appointed a Data Protection Officer (DPO) in compliance with Article 37 of the General Data Protection Regulation.

The Data Protection Officer plays a key role in ensuring accountability, but is not solely responsible.

2. Purpose

This policy outlines the strategic framework for managing and supporting information governance within the council. It describes both the roles and responsibilities of those who are tasked with overseeing that information governance is appropriately supported, as well as detailing the information governance responsibilities of all staff.

The council will ensure that:

- Regulatory and legislative requirements are met;
- Confidentiality of information is assured;
- Information is protected against unauthorised access;
- Quality and integrity of information is maintained;
- Business continuity plans are produced, maintained and tested;
- Information governance training is available to all staff;
- Information security breaches are investigated; and
- The mandatory requirements of the annual Data Security and Protection Toolkit are met.

The council has 'privacy by design and default' at its forefront. An information risk assessment process has been established, supported by the Information Management Service (IMS), who are able to provide advice throughout the process. This process is linked to the procurement, supplier assessment and contract management processes.

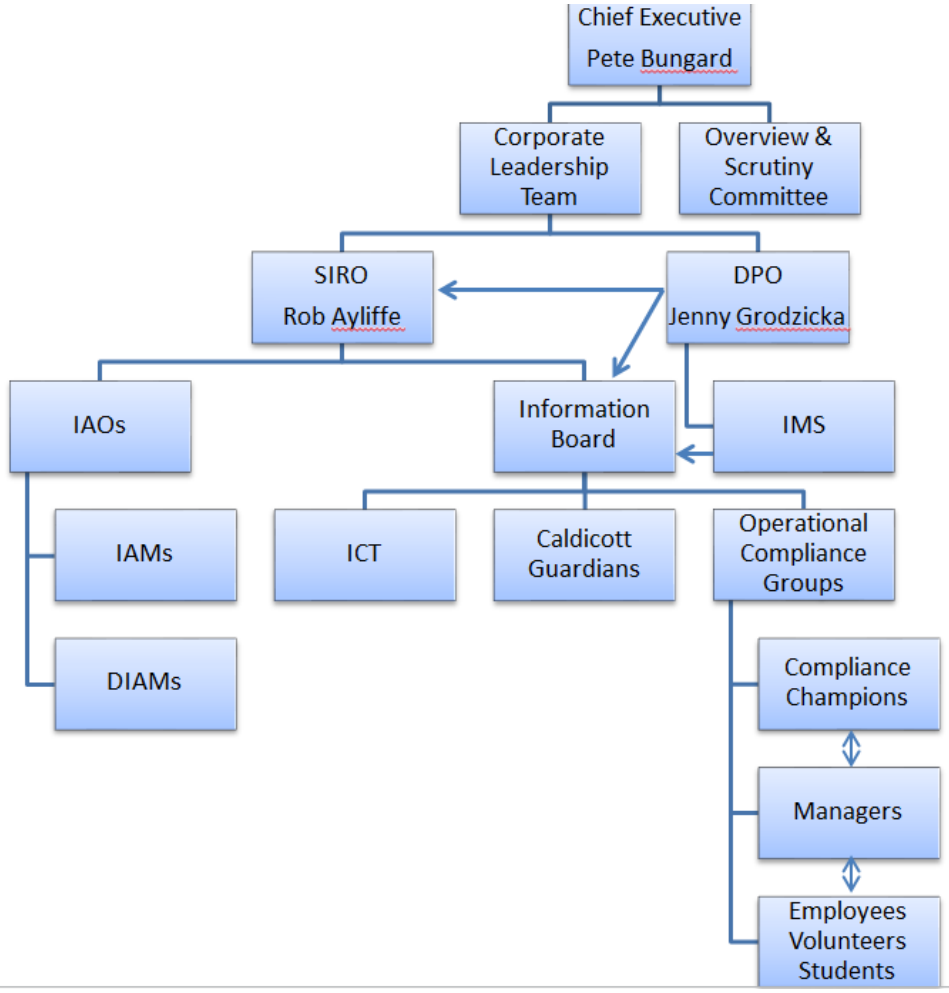
The council is also committed to being transparent with the public and users of its services. Required changes to privacy notices are also identified and implemented through the information risk assessment process.

3. Scope

This policy applies to all employees, partners, contractors, agents of the council and other third party users (including volunteers, students and those on work experience placement) who require any form of access to the council's information (whether in paper or electronic form) and information systems.

This policy should be adhered to at all times when accessing information in any form and from any device. Questions regarding the content or application of this policy should be directed to informationsecurity@gloucestershire.gov.uk or 01452 324000.

4. Roles & Responsibilities



All users are bound by the council's Code of Conduct for Employees to maintain the confidentiality of the information they access; and must not use the information for unauthorised purposes.

The **Chief Executive** has overall accountability for information governance.

Overview & Scrutiny Committee carries out the scrutiny functions of the council, providing a corporate overview of performance, the budget, risk management, compliance and service improvement.

The **Corporate Leadership Team** (CLT) has oversight of information governance, and members are responsible for supporting initiatives within their directorates and service areas. CLT also has responsibility for corporate planning and making business decisions which might impact on how the council processes personal information, ensuring the DPO (or representative) is involved in those decision making discussions.

The **Senior Information Risk Owner** (SIRO) is responsible for managing information risk at the highest level, and takes a holistic approach to information risk across the council. Alongside the DPO and IAOs, the SIRO is also responsible for ensuring the council's business processes and decision making are in line with GDPR and good practice. The SIRO at the council is Rob Ayliffe, Director of Policy Performance & Governance.

The **Data Protection Officer** (DPO) is a statutory role set out within the General Data Protection Regulation (GDPR), and is responsible for helping the council fulfil its data protection obligations through advice and monitoring. The requirements of Article 39 of the GDPR are included in the DPO job description. The DPO is accountable to the council's CLT.

The council has appointed an internal, existing employee as its DPO. As DPO and Head of Information Management, the tasks and focus of each role complement each other, and do not conflict. Neither responsibility is focused on determining the purposes and means of processing personal data but both are focused on providing advice about the risks, mitigations, safeguards and solutions required to ensure the council's processing is compliant and supported by its business decisions. Where the advice of the DPO is not followed, this is documented.

The DPO's contact details are included within the council's privacy information and records of processing activities. There is a dedicated email address and monitored inbox for data protection queries or complaints received internally or externally. The DPO at the council is Jenny Grodzicka, Head of IMS (DPO). The DPO can be contacted on dpo@gloucestershire.gov.uk or 01452 324000

The DPO is also the council's contact with the Information Commissioner's Office in its capacity as UK supervisory authority. They maintain independence and are able to raise issues in the way and with the forum they see fit, without approval from their line manager.

The **Information Board** is chaired by the SIRO and provides overall direction and leadership for information governance arrangements, ensuring appropriate governance, policy and standards are in place across the council.

The **Caldicott Guardians** are senior managers responsible for protecting the confidentiality of service users' health and care data and making sure it is used appropriately, acting as the 'conscience' of the organisation and championing confidentiality issues with senior management. They also provide informed guidance on complex matters involving confidentiality and information sharing.

Information Asset Owners (IAOs) are senior managers responsible for managing the risks to their information assets.

Information Asset Managers (IAMs) are operational managers responsible for information assets on a day to day basis.

Delegated Information Asset Managers (DIAMs) act as a contact for IMS for information governance queries or information security breach investigations. A DIAM may be delegated the responsibilities of an IAM.

The **Information Management Service (IMS)** provides a lead for the council on all aspects of information management, including governance, security, records management and compliance.

Their approach has 'privacy by design and default' at its forefront. They have an established privacy assessment process led by the Data Protection Officer, who is available to provide advice throughout the process. This process is linked to the council's procurement, supplier assessment and contract management processes.

IMS is also responsible for maintaining the council's key accountability documentation, including a Record of Processing Activity (ROPA), Corporate Retention Schedule and Information Asset Register.

Directorate operational compliance groups discuss service level data protection, records management and information securities issues, and also act as a conduit to and from the Information Board, providing oversight of how data protection legislation is complied with at an operational level.

Information Compliance Champions sit within each Directorate, promoting good practice and assisting senior managers in ensuring compliance with GDPR and data protection legislation across their service area.

Managers are responsible for implementing this policy and associated policies in their teams, and identifying and raising information risks with the relevant Information Asset Owner.

Any manager with responsibility for volunteers/students/work experience placements must also ensure these individuals are fully aware of their need to comply with this policy and its associated policies when accessing council information, and manage their access accordingly.

Employees are responsible for understanding and complying with this policy and associated policies. Failure to comply with this policy or associated policies may result in disciplinary action.

Contractors and third party suppliers are responsible for complying with this policy and associated policies in line with their contract or agreement. Failure to comply may result in the termination of their contract or agreement.

Volunteers/students/individuals on work experience placements are responsible for understanding and complying with this policy and associated policies. Failure to comply may lead to the immediate termination of their placement with the council.

5. Training

All staff must complete the corporate training, both as part of their induction to working at the council and on an annual basis, thereafter. This includes, but is not limited to:

- Induction training, to be completed within 3 months of their commencement at the council
- Monthly information security videos
- Annual refresher training

All staff must also watch mandatory monthly Information Security e-learning videos. At least 95% of all staff will have completed relevant training in the period 1 April to 31 March each year.

The Information Management Service will review training needs on a regular basis to identify specific data security and protection training for the key roles supporting the information governance agenda.

Members of the Information Board, including the SIRO and Caldicott Guardians, will undertake appropriate data security and protection training on a regular basis.

Information Asset Owners and Information Asset Managers must undertake relevant annual training to understand their roles and responsibilities.

Tailored awareness sessions will be provided to teams on a needs basis, and regular articles on information governance topics will be published through corporate communication channels.

6. Related policies

This policy should be read in conjunction with the Information Management and Security suite of policies which can be found on the council's information management and security policies webpage. Members of staff should also refer to the council's Code of Conduct.

7. 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)
Owner:	Jenny Grodzicka, Head of IMS and DPO
Approval body	Information Board
Document Number:	v1.0

Revision History

Revision date	Summary of Changes	Changes marked

Approval History

Version	Approval Body	Date
v1.0	Information Board	December 2020