Scottish Courts and Tribunals Service

Information Governance Principles

Issued by Information Governance and Correspondence Team, Scottish Courts and Tribunals Service

Document Control

Date of Approval	
Version Number	**1.2**
Review Frequency	**Annual**
Next Review Date	**January 2026**

Contents

1. Executive Summary

The Scottish Courts and Tribunals Service (SCTS) is responsible for providing administrative support to Scotland's courts, devolved tribunals, their judiciary and the Office of the Public Guardian. As such SCTS is custodian of a vast amount of sensitive and confidential information about individuals, companies and other organisations. . To ensure the protection of this information and the effective functioning of the justice system, the SCTS must have a robust set of information governance principles in place.

These principles outline the SCTS' commitment to ensuring the confidentiality, integrity, and availability of all its information assets. They set out a comprehensive framework for information governance, covering all aspects of SCTS operations, from data management to compliance with data protection legislation and the Public Records (Scotland) Act 2011.

These principles align with the strategic priorities of the SCTS in particular:

- Well Supported Judiciary
- Purposeful Collaboration
- Digital Services
- Efficiency & Best Value
- Satisfied Service users

2. Our Information Governance Principles

To maintain effective information governance the SCTS observes the following five principles:

- We protect the confidentiality, integrity, and availability of all our information assets.
- We comply with all applicable data protection legislation.
- We ensure that SCTS information is used effectively and efficiently to support the organisation's key functions and strategic priorities.
- We manage SCTS information risks effectively.
- We educate and inform SCTS staff about their information governance responsibilities.

3. Key Controls and Actions

In order to support delivery of, the SCTS has a range of measures in place and a rolling plan of action for improvement. Over the course of 2025/26 the organisation will focus on the following actions:

3.1 Maintain and develop a robust set of information governance and records management policies.

The SCTS will refresh and develop a new set of information governance and records management policies supporting the development of systems and procedures that comply with current legislation.

3.2 Implement a comprehensive business classification system and records taxonomy.

The SCTS will implement a comprehensive business classification system and records taxonomy through the development of a centralised records management system within the SCTS.

The SCTS currently maintains a devolved system of records management. Each business unit is responsible for its own records management, setting many of their own policies, procedures and enforcing these. Centralising this function will allow the SCTS improve arrangements and ensure it fulfils its statutory obligations.

This function will be centralised and managed by the Information Governance and Correspondence Team (IGCT).

3.3 Strengthen data access controls and monitoring.

The principle of Rule Based Access Control will be used to maintain the security of access and manage the audit trail for information. Whilst an Open Data Framework approach is the best approach, some files will need to have restricted access such as CEO office restricted files, management files and departmental budget folders. Where these restrictions are required then the Privacy by Design principles will be followed.

3.4 Regularly review and update information governance procedures.

Information governance processes and procedures need to be regularly reviewed and updated to accommodate changes in legislation and technology that is used by the SCTS. The SCTS also needs to ensure that the Records Management Plan that is submitted to National Records of Scotland is current, compliant and fit for purpose.

Over the course of this year the IGCT will review the policies, processes and procedures in place to ensure these align with industry best practice, the regulatory requirements placed upon the SCTS and the SCTS Records Management Plan.

3.5 Provide regular training and awareness-raising for SCTS staff.

SCTS has a range of both information governance resources and training materials in place. Over the coming year the IGCT will work to produce improved training materials and courses to aid understanding of the importance of good and accurate record keeping. These will cover statutory requirements and the implications of poor records management and information governance. The IGCT will work with the Education and Learning Unit (ELU) to develop further material on data breaches and materials that will support the rollout of SharePoint as a records repository enabling staff to be fully trained on its use.

3.6 Leverage technology to support information governance.

The SCTS will explore and – where beneficial - use the following technologies to further support and enhance its information governance and records management policies and procedures.

3.6.1 Artificial Intelligence: The SCTS will leverage artificial intelligence (AI) to improve its information governance. AI can help automate the classification and retention of information, reducing the risk of human error and ensuring compliance with legal and regulatory requirements.

We will focus on the use of ethical AI as defined below:

'*Ethical AI refers to artificial intelligence systems that are designed and developed with the principles of accountability, transparency, privacy, and individual human rights in mind. It is a set of guiding principles that stakeholders, from engineers to government officials, use to ensure that AI technology is developed and used responsibly.'*

The use of ethical AI links with the Open Data principle as it demonstrates transparency in decision making. Due to the obligations the SCTS has under the Freedom of Information Act 2000, it is required to produce an audit trail of decisions made and the reasoning behind these. The use of ethical AI systems as opposed to more opaque AI systems supports this.

3.6.2 Cloud Computing: The SCTS will migrate its information to cloud-based platforms to improve accessibility and collaboration. Cloud computing can provide secure access to information from anywhere, at any time, and on any device.

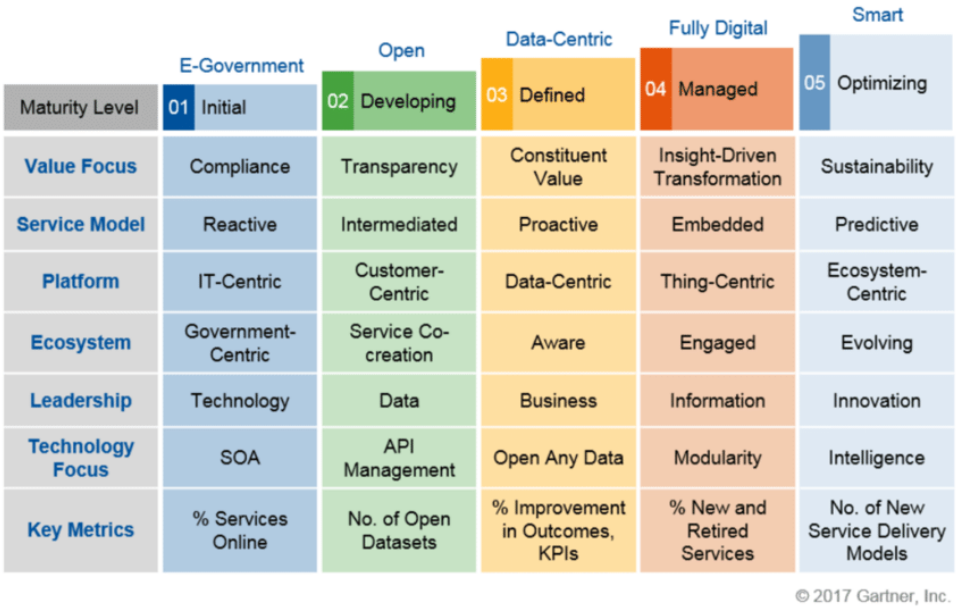
3.6.3 Data Analytics: The SCTS will use data analytics to gain insights into its information and improve decision-making. Data analytics can help identify patterns and trends in information, enabling the SCTS to make informed decisions about its information governance strategy.

The data analytics used by IGCT will be driven by the reporting tools that are included in M365 and any further enhancements to them.

3.6.4 Digital Preservation: The SCTS will implement digital preservation strategies to ensure that, where applicable, information is preserved for future generations. Digital preservation can help ensure that information is accessible and usable over time, even as technology changes.

3.6.5 Open Data: The SCTS will explore the use of open data to improve transparency and accountability.

An **Open Data Framework** is a set of principles, policies, and practices that enable the sharing of data in a way that is accessible, discoverable, and can be used by anyone. It is designed to promote transparency, accountability, and collaboration between governments, businesses, and individuals. The Open Data Maturity Model described by Gartner is a way to assess how well an organisation publishes and consumes open data, and identifies actions for improvement. The model is based around seven themes and five progress levels.

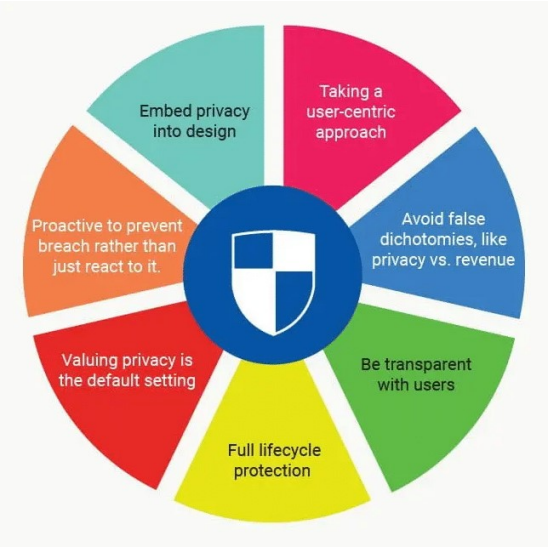


	E-Government	Open	Data-Centric	Fully Digital	Smart
Maturity Level	01 Initial	02 Developing	03 Defined	04 Managed	05 Optimizing
Value Focus	Compliance	Transparency	Constituent Value	Insight-Driven Transformation	Sustainability
Service Model	Reactive	Intermediated	Proactive	Embedded	Predictive
Platform	IT-Centric	Customer-Centric	Data-Centric	Thing-Centric	Ecosystem-Centric
Ecosystem	Government-Centric	Service Co-creation	Aware	Engaged	Evolving
Leadership	Technology	Data	Business	Information	Innovation
Technology Focus	SOA	API Management	Open Any Data	Modularity	Intelligence
Key Metrics	% Services Online	No. of Open Datasets	% Improvement in Outcomes, KPIs	% New and Retired Services	No. of New Service Delivery Models

3.6.6 Privacy by Design: The SCTS will continue to adopt a privacy-by-design (PbD) approach to its information governance principles. This means that privacy considerations will be integrated into all aspects of the SCTS information governance strategy. This includes the design of new systems and the implementation of new policies and procedures. The goal of PbD is to prevent data privacy breaches and protect the privacy of individuals by proactively incorporating data privacy safeguards into systems and processes.

The **UK GDPR** requires organisations to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is known as data protection by design and by default**.**

Privacy by Design can be represented by the seven principles below



Source 7 Key Principles of Privacy by Design for Businesses

3.6.7 **User-Centred Design (UCD)**: The SCTS will adopt a user-centred design approach to its information governance principles. This means that the needs and preferences of users will be taken into account when designing new systems and processes.

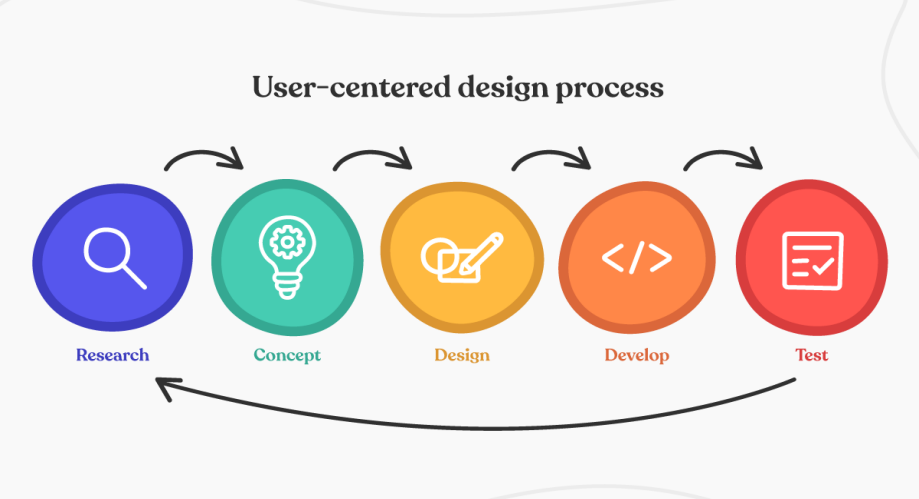
UCD is an iterative design process where designers focus on the users and their needs in each phase of the design process. This is done through a variety of research and design techniques, to create highly usable and accessible products for them.

The UCD process typically involves five distinct phases:

- understanding the context in which users may use a system,
- identifying and specifying the users' requirements,
- defining those requirements,
- developing solutions, and
- evaluating the outcomes against the users' context and requirements, developing iterative improvements based on that feedback.

This process aligns with the Understand, Incubate, Develop and Deploy stages of the LOAD framework used to develop and deliver new systems and business change within the SCTS.

The UCD design process is summarised in the diagram below.



Source: A Beginner's Guide to User-Centred Design | WowMakers

UCD considers the whole user experience and involves professionals from across multiple disciplines, such as software and hardware engineers, domain experts, stakeholders, and the users themselves.

4. How we will manage and monitor progress

Strong stakeholder engagement and the importance of measuring key metrics annually to establish a baseline and trends are recognised as essential to managing and monitoring progress. In addition we recognise the particular threat posed by cyber security and have specific goals set to maintain and improve performance in this area. A summary of each of these elements is provided below.

4.1 Engaging with stakeholders to ensure alignment with information governance goals.

IGCT will engage with business units across the SCTS as well as external stakeholders such as National Records of Scotland to develop and maintain systems and processes that are fit for purpose and legally compliant, whilst fulfilling operational requirements. This will be achieved through the creation of a collaborative working environment, which will also help to develop knowledge and understanding in this area which should in turn lead to a reduction in data breaches. This aligns with the User Centres and privacy focused design approaches outlined in section 3.

4.2 Focusing on Cyber Security.

The SCTS recognises the importance of information security and will use new technologies to enhance its cyber security readiness. This includes the use of advanced encryption, multi-factor authentication and other security measures to protect its information. The Cyber Security Team will take forward this work and the implementation of necessary security policies.

Cyber Security goals

- To define, establish and incrementally increase the maturity of cyber security services that are required of an organisation of the size, complexity and importance of SCTS.
- To ensure SCTS is managing and, where appropriate, materially reducing risk and can readily demonstrate so.
- Date breaches caused by cyber-attack are minimised in terms of both likelihood and impact.
- Cyber security related audit exercises can be undertaken smoothly, with little specific effort to generate evidence and with few unexpected findings.
- SCTS routinely achieves targeted accreditations on an annual basis such as
    - Cyber Essentials Plus,
    - Cyber Resilience Framework to a target level

4.3 Performance Measurement

The SCTS will measure its progress in achieving its information governance principles through the following indicators. These are periodically measured and reported on, with reports being reviewed by the SCTS Executive Team and information relating to incidents, breaches and training overseen by the SCTS Board and its relevant Committees.

- The number of security incidents.
- The number of data breaches and data loss incidents.
- The level of staff compliance with information governance policies and procedures and completion of mandatory e-learning.
- The effectiveness of data access controls.
- The level of stakeholder engagement with information governance activities.

The SCTS will review its information governance principles 12 months after publication to ensure it remains relevant and effective.

5. Conclusion

Effective information governance is essential for the SCTS to fulfil its functions. It can:

- Improve access to information for judges, court staff, and the public.
- Reduce risk of information loss or breaches.
- Enhance decision-making and operational efficiency.

- Increase public trust and confidence in the SCTS

These Principles and associated actions present a roadmap to achieving this goal, ensuring that information is managed effectively for the benefit of all stakeholders.

By implementing the principles, the SCTS can use the power of information to improve its operations, enhance transparency, and ensure the best possible service.