Information management policy

2. Version 1.1
3. 17 September 2021
4. Departmental Records Officer & Information, Governance and Complaints Officer

Information management policy

Table of contents

1. Version Control Version	Date of publication	Reason for amendment
1.0	13 September 2021	Draft for consideration at the Management Team meeting 17 September 2021
1.1	17 September 2021	Minor consequential amendments after discussion at the Management Team meeting
1.2	22 May 2023	Draft for consideration at the Management Board meeting XX 2023

2. Purpose

2.1 This document establishes the approach of the Supreme Court of the United Kingdom to managing its data.

2.2 The document explains the concept of “Information Asset” and outlines the roles of “Information Asset Owner” who takes responsibility for each Information Asset.

2.3 This document also defines the primary responsibilities of an Information Asset Owner (IAO) in managing the risks to personal data held within a department.

2.4 The document establishes the roles and responsibilities of the Senior Information Risk Owner (SIRO) in supporting IAOs and ensuring good practice with regards to information management.

2.5 This document outlines the role of the Accounting Officer (AO) who has oversight of all information security.

2.6 The Supreme Court uses the Information Asset Register (IAR) to record processing activities to help ensure we meet our obligations under the Data Protection Act 2018.

3. Background

3.1 The Supreme Court holds and manages information in a variety of formats. It is vital that the Court understands the information it holds and the purposes for which it is held so that IAOs can be proactive in managing and protecting it.

3.2 Having a proactive and responsive IAR and Information Management Policy ensures that the Court is aware of all data it holds in relation to how the Court functions, outlines who is responsible for the information and how its data and assets can be used.

3.3 Good information management aligns with the Court's strategic priorities to ensure effective administration and delivery as outlined in the administration Business Plan.

3.4 IAOs are supported by the SIRO to ensure that they are accountable for the collection, processing and protection of information stored within the organisation.

3.5 The Court takes its responsibilities seriously and ensures that the right levels of security and protection are applied to all information we handle. This policy outlines the commitment of the organisation to manage information securely and professionally in line with the seven principles outlined in the General Data Protection Regulation (GDPR):

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

3.6 It is the responsibility and duty of all IAOs and the SIRO to adhere to the above principles and ensure that all information is handled within these parameters. Effective information management protects our customers and any information they share with the Court.

3.7 This process is limited to the administrative functions of the Court and the Information Asset Owners who process information on behalf of the Court.

3.8 With regards to judicial processing of information, there are exemptions contained within the Data Protection Act 2018 which limit, at least in part, the disclosure obligations that can apply.

4. Definitions, roles and responsibilities

Responsibilities

4.1 All permanent and temporary employees, contractors, consultants and secondees who have access to the Court's records, working on behalf of the Court or on Court business are responsible for managing records, wherever these records are and whatever form they are in.

4.2 The Court owns all records created by employees carrying out Court business-related activities. Unless the originator asserts ownership, records received by staff are also owned by the Court. Individual employees do not own records; however, they are responsible for managing them.

Definitions

4.3 **Records** are defined following ISO standard ISO 15489 – 1 as information created, received and maintained as evidence and information by an organisation or person in pursuance of legal obligations or in the transaction of business

4.4 **Retention** usually means the length of time for which records are to be kept. It normally represents and will be expressed as a disposal period

4.5 **Disposal** includes any action taken or yet to be taken to determine the fate of records including destruction and transfer to a permanent archive

Information Asset

4.6 In order for the Supreme Court to understand its information, and how to manage and protect it, it is vital that is it understood what is meant by the term 'information asset'.

"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles".

4.7 Information assets form a detailed body describing the function, role and content of this information. Information assets are recorded in the Information Asset Register. All information assets can carry risk and should be managed appropriately along with an accurate and timely retention schedule which indicates how long the asset should be retained before its disposal.

4.8 Information assets can be physical (e.g. paper) or digital. Digital information and records are anything that exists in a digital or electronic media, e.g. computer files, emails, database contents. It includes both 'born digital', which were created in digital formats, and digital versions of physical documents (e.g. scans)

Information Asset Register

4.9 An Information Asset Register (IAR) is a working document used for establishing and managing the Court's information assets and any potential risk.

4.10 The IAR functions as a record of all current IAO's and their attributed information assets. The IAR is reviewed and updated quarterly by the DRO and Information, Governance and Complaints Officer in collaboration with IAOs. A quarterly assurance statement from each IAO to the SIRO is required.

Roles

Accounting Officer

4.11 The ultimate responsibility for information security for the Supreme Court lies with the Chief Executive in their role as the Accounting Officer (AO).

4.12 The AO role involves:

- Ensuring that information risks are assessed
- Ensuring that risks are mitigated to an acceptable level within the organisation.

4.13 As part of the annual Statement of Internal Control Procedures, the AO must complete an Annual Assessment of Information Risk Management.

Senior Information Risk Owner

4.14 The Senior Information Risk Officer (SIRO) for the Supreme Court is the Director of Corporate Services.

4.15 The SIRO role involves:

- Being accountable for management of assets within the organisation
- Owning associated risks and setting risk appetite within the organisation
- Managing access controls for access to assets
- Ensuring all staff in their area receive appropriate information management training for their role
- Ensuring all delegated responsibilities are executed appropriately and to time
- Functions as an escalation point for IAO's

Information Asset Owners

4.16 The Information Asset Owners (IAOs) should understand the aims of the organisation and strategic priorities, and in turn how information assets contribute to these aims.

4.17 The role of an IAO includes:

- Recording and removing assets from the Information Asset Register according to the lifecycle of the asset
- Managing the asset(s) risk along with recording any changes to the asset
- Escalating and reporting risks
- Providing formal reporting to SIRO on risks and assets
- Taking responsibility for use, transfer, controls of the assets
- Recording incident management reports relating to the assets
- Determining the value of the asset to the organisation and the appropriate course of action for the asset

Departmental Records Officer

4.18 The Departmental Records Officer (DRO) is responsible for:

- making sure that departmental records are stored securely

- making sure that the lifecycle of records is managed appropriately
- making sure that the information management policies are kept up to date and relevant to the needs and obligations of the Court, consulting and working with Court staff and the appropriate external regulatory bodies
- informing staff about the information management policy, and for ensuring that all staff are aware of their responsibilities for managing records
- giving information management advice and guidance to IAOs
- taking over management of information assets for which there is no clear responsible business area

5. Personal information

What information do we hold?

5.1 The Supreme Court holds information regarding its staff, contractors and Justices.

5.2 The Supreme Court holds information regarding our users. Personal data is information supplied by an individual that can be used to identify them, for example, name, address, date of the birth.

5.3 The Supreme Court may hold information regarded as special categories of personal data. This is information regarding a persons' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data (where used for identification purposes), data concerning health, sex life or sexual orientation.

5.4 Information includes but is not limited to case records, internal and external correspondence, contact details.

What do we mean by processing?

5.5 All information held by the Supreme Court is processed lawfully, fairly and in a transparent manner. All information assets are recorded on the IAR.

5.6 Personal information is processed in line with the judicial functions of the Court and the administrative functions of the Court. This includes collection, storage, retention and destruction. All information collected is managed by the relevant team responsible and

retained until there is no further use for the information. It will then be destroyed or archived as per the Records Retention Schedule.

5.7 Judicial functions may include notes taken during court or hearings, drafting and/or published orders or judgments. Information of this nature would be exempt from disclosure.

What are my rights under GDPR?

5.8 GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

5.9 To request a copy of any personal information the Court may hold on you please contact: data.protection@supremecourt.uk

5.10 A request for personal information is commonly known as a Subject Access Request. Guidance on making a SAR can be found on the Information Commissioner's Office website.

5.11 Members of the public can request recorded information held by the Court that is not related to an individual (for example, administrative processes by the Court). This information is accessible via the Freedom of Information Act. Please contact: foi@supremecourt.uk

Exemptions

5.12 In certain circumstances, the Data Protection Act 2018 provides exemptions from GDPR provisions. Information processed in accordance with the judicial functions of the Court is a listed exemption and the legislation is reproduced at paragraph 6.2 below. A comprehensive guide to exemptions can be found on the Information Commissioner's Office website.

5.13 Data Protection Act 2018: Schedule 2 Paragraph 14

Judicial appointments, judicial independence and judicial proceedings

14

(1) The listed GDPR provisions do not apply to personal data processed for the purposes of assessing a person's suitability for judicial office or the office of Queen's Counsel.

(2) The listed GDPR provisions do not apply to personal data processed by:
(a) an individual acting in a judicial capacity, or
(b) a court of tribunal acting in its judicial capacity

(3) As regards personal data not falling within sub-paragraph (1) or (2), the listed GDPR provisions do not apply to the extent that the application of those provisions would be likely to prejudice judicial independence or judicial proceedings.

6. Storage of information assets

6.1 All information assets must be stored in approved corporate storage locations. This means:

- registered paper files
- SharePoint / Teams sites
- centrally owned archive storage
- contractually established off-site storage locations

6.2 Information that does not form part of the record of the Court's activities, or is not of ongoing business value, should be deleted as soon as it is no longer required in line with the Record Retention Schedules that apply.

Account-specific storage

6.3 Departmental information should not be stored in account-specific storage, i.e. Outlook and OneDrive accessible only by an individual.

6.4 OneDrives should be used for storing business-related personal documents, e.g. HR and performance related documents. Documents of business value (including drafts) must

be saved to a corporate storage location, to ensure that business continuity can be maintained.

6.5 Outlook should be used for short-term storage of communications and ephemeral information. Records of business decisions stored in emails should be transferred to a corporate storage location.

6.6 All data in account specific storage remains searchable by and accessible to the Departmental Records Officer on the basis of corporate need. Should such a need arise, a written request must be made to the SIRO who shall has the authority to authorise any searches that may be needed or specify any conditions that must be adhered to.