Scottish Civil Justice Council: Records Management Plan

Scottish Civil Justice Council Records Management

1. The Scottish Civil Justice Council (SCJC) was established on 28 May 2013 under The Scottish Civil Justice Council and Criminal Legal Assistance Act 2013. The functions of the SCJC include the preparation of draft rules of procedure for the civil courts and providing advice and making recommendations to the Lord President on the development of the civil justice system in Scotland.

2. In conducting its business, the SCJC is guardian to a range of information, including in relation to its own and others' consideration of draft rules, improvements to the civil justice system and proposals for reform. The SCJC is also guardian to a variety of corporate records, including as to appointments, expenditure, management information and staffing. Some of this information is both sensitive and personal in nature.

3. In the event that any circumstances arise which are not covered by the procedures and policies outlined in this document, Scottish Court Service (SCS) records management policies will apply.

Commitment

4. The SCJC will ensure that information is handled responsibly, stored securely, and that thought is given to the risks of sharing information with others and when the information is no longer required, it will dispose of it appropriately and securely.

5. The SCJC became subject to the provisions of The Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIRs) on 28 May 2013. The SCJC will ensure that it upholds its duties with respect to its obligations under FOISA and the Data Protection Act 1998 and that its records are stored in a manner which facilitates the easy and speedy retrieval of information.

Preservation and archiving

6. It is essential that records of decisions and actions are complete and accurate. Details relevant to decisions or actions, including minutes and correspondence, will be retained in accordance with the preservation and retention schedule at Annex A.

7. All records (including those of an electronic nature) subject to the preservation schedule will be stored in conditions conducive to their long term maintenance and preservation until such time as they are required to be made available for

transmission to the National Records of Scotland (NRS). Retention periods and modes of transmission will be the subject of periodic review.

8. All records subject to preservation and retention schedules will be stored in hard copy, except where the medium of the record renders this not possible. An electronic records database which mirrors the physical files will, however, be maintained.

Transmission of record to NRS

9. Records that need to be preserved will be archived after 5 years. The NRS takes transmission from SCJC of records over 10 years old or in the case of electronic records, over 5 years old.

10. When preparing records for transmission to NRS, the access status of the records will be reviewed, to determine:

- which information must be available to the public (ie made 'open') on transfer because no exemptions under FOISA or the EIRs apply;
- which information should be withheld from public access through the application of an exemption under FOISA or an exception under the EIRs; and
- consider whether the information must be released in the public interest, notwithstanding the application of an exemption under FOISA or an exception under the EIRS.

11. Records to be transmitted to NRS will be archived in the SCJC filing room at Parliament House.

Destruction Arrangements

12. The SCJC will adhere to the destruction arrangements in place within the SCS.

13. All information which is not subject to a preservation and retention schedule and has outlived administrative usefulness will be destroyed in a secure manner. Information Assets that are protectively marked will be disposed of by using the following:

- cross cut shredder;
- confidential waste bag/sack; or
- special arrangements for the disposal of confidential material made through Departmental Security.

14. All corresponding electronic files and documents will be deleted in tandem.

15. Certain records are designated for destruction after specified periods, which are calculated from the date of the last entry in that record. A member of the Secretariat with allocated records management duties will be responsible for arranging for the destruction of these records.

16. The Secretariat will make arrangements for disposal of documents in the possession of SCJC or committee members where necessary.

Records review

17. A file must become closed and subject to destruction (or retention procedures):

- if 5 years have lapsed since the first paper was placed in the file;
- if the subject matter is no longer current;
- if papers have not been added to the file for at least six months and/or the file has become too bulky (over 4cm in width).

18. An annual review of electronic and physical files will be undertaken by the SCJC Secretariat. A file can be reviewed up to four times in its existence.

19. There are several options for the disposal of each file. The disposal option must be marked clearly on the front cover of the file:

- **Destroy-** upon closure of file, or at 1st or 2nd review.
- **Preserve for NRS**- mark for future preservation by NRS
- **Retain in branch-** the file has continuing and regular administrative use. These files must be reviewed every 10 years.
- **Forward Destroy**- the file is to be destroyed at a future date which is to be specified by the reviewer.
- **First Review**- 5 years after closure of the file.
- **Second Review**- when a decision is not obvious at the first review, the file is marked for a second review. The ideal date for the second review is around 15 years from the date of the first document being placed in the file but should be no longer than 25 years.

Information Sharing

20. The Lord President's Private Office (LPPO) provides legal advice to the SCJC. The SCJC and LPPO will share files where appropriate to avoid duplication and to assist the SCJC to meet its obligations under FOISA. Where legal advice is routinely provided, LPPO will maintain corresponding files, where relevant records will be stored in accordance with legal and professional obligations.

21. The SCJC Secretariat will be responsible for maintaining SCJC electronic and physical files.

22. On occasion, information may be shared with other organisations. The basis on which such information should be shared and how it should be handled will be considered on a case by case basis in conjunction with the other party/parties.

Filing

23. The paper file constitutes the official corporate record. However, in order to facilitate the easy and speedy retrieval of information, electronic files will be maintained. All electronic files which replicate the official corporate record must mirror the physical file.

24. The SCJC Secretariat and staff of the LPPO will utilise an agreed naming convention for all files and electronic records. This should contain at a minimum, the date (in YYMMDD format) followed by a brief description of the subject matter, the nature of the document and, in the case of correspondence the details of sender and recipient and reference.

Protective markings

25. The SCJC will classify information in accordance with the Protective Marking levels used by the SCS. These are:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED
- PROTECT

26. The Protective Marking to be applied to any information will be determined primarily by reference to the consequences that are likely to result from the compromise of that information. A guide to protective markings is provided at Annex B.

27. The SCJC also uses the protective marking PRIVATE for SCJC and committee meeting papers which are not to be routinely published. Documents with a PRIVATE marking should not be circulated to external parties.

28. It is the responsibility of the originator to determine the protective marking that should apply to the information, based on an assessment of the sensitivity of its content and the impact of its compromise. Where information received is unclassified, the SCJC Secretariat will make an assessment and apply any protective marking required, in consultation with the sender where appropriate and/or necessary.

Responsibilities of SCJC and committee members and staff

29. Council and committee members and SCJC staff will observe the following principles:

- Personal data and information should be protected with care and vigilance.
- Protective markings should be observed and understood and protectively marked documents should be handled in accordance with the relevant handling guidelines.
- Information and data, whether held electronically or physically should be stored securely.
- Access to equipment and media on which SCJC records are stored should be password protected and all passwords should be chosen carefully and should not be disclosed to anyone.
- Information or data which is not already in the public domain should not be released without the Chairman's permission, or without otherwise having the authority to do so.
- Care should be taken when working outside, making sure that confidential papers or conversations are not seen or heard by others.
- Information and data should not be unnecessarily transferred or transported.

30. SCJC staff will undertake all relevant information and data handling training and familiarise themselves with the SCS 'Information Risk Management Policy'.

IT Arrangements

31. Members of the SCJC Secretariat all have access to SCS IT systems in order that they may carry out their functions effectively.

32. Access to IT is password controlled and staff members will be instructed that all passwords be chosen carefully and not disclosed to any other person. PCs and laptops should be logged out or "locked" when not in use and portable media should be suitably encrypted. Internal emails containing information of a sensitive nature will be identified as such with an appropriate protection marking in the subject field.

Reporting Procedures

33. Any incident which might compromise the confidentiality, integrity or availability of information will be reported internally as soon as discovered and reported to the Secretary or Deputy Secretary to the SCJC.

34. Records and information will at all times be processed and handled in accordance with the requirements of the SCJC Records Management Plan.

Preservation and Retention Schedule

1. The table below outlines a schedule for retention of SCJC records.

Type of File	Instruction	Notes
SCJC AND COMMITTEE PAPERS		
Agendas, meeting papers (including private papers), minutes.	Preserve- to go to NRS after 10 years	
Records on establishment of committees, and working groups (remit, membership etc.).	Preserve- to go to NRS after 10 years	
APPOINTMENTS		
Appointment letters and supplementary documentation	Preserve- to go to NRS after 10 years	
Subsequent records	Destroy- after 15 years (or period appropriate to length of appointment and possible reappointments)	
LEGISLATION		
Draft rules created at request of SCJC or its committees and supplementary documentation.	Preserve- files to go to NRS after 10 years	1st Review if subject likely to be 'live' or still under consideration.
Records relating to consideration of new or amendments to primary and secondary	Preserve- files to go to NRS after 10 years	

Type of File	Instruction	Notes
legislation.		
Records containing copies of documents originating outwith the SCJC or its committees.	Destroy- 5 years after closure	
FINANCE		
Payment records: invoices for catering, hospitality, consultancy etc.	Destroy- 7 years after closure	
Estimates	Destroy- 10 years after closure	
Account records	Destroy- 10 years after closure	
GENERAL CORRESPONDENCE, BRIEFINGS AND MEETINGS		
Casework on FOISA, EIR and Data Protection requests.	Preserve- to go to NRS after 10 years.	1st review if records contain precedent material.
General correspondence	Destroy- 5 years after closure	
Official briefings.	Preserve- to go to NRS 10 after 10 years.	
Routine meeting and visit briefings	Destroy- 5 years after closure	
Non-routine meeting and visit briefings	1st Review.	
POLICY DEVELOPMENT		

Type of File	Instruction	Notes
Files on subjects of interest to but not the direct responsibility of, the SCJC (e.g information on initiatives by other organisations).	Destroy- after 5 years after closure	
Records, such as public statements, outlining decisions of or recommendations by the SCJC (including committees).	Preserve- to go to NRS after 10 years	1st Review if subject likely to be 'live' or still under consideration.
Liaison with external agencies, e.g. documents laid before Parliament (including written evidence). correspondence or reports provided to government or other bodies, responses to consultations by other bodies, etc.	Preserve- to go to NRS after 10 years	1st Review if subject likely to be 'live' or still under consideration.
SCJC commissioned research	Preserve- to go to NRS after 10 years.	1st Review if subject likely to be 'live' or still under consideration.
Consultation responses, consultation analysis and reports	Preserve- to go to NRS after 10 years	
GOVERNANCE AND CORPORATE DEVELOPMENT		
Standing Orders, protocols and supporting documentation, corporate policies (eg	Preserve- to go to NRS after 10 years	

Type of File	Instruction	Notes
FOISA).		
Office procedures, management planning, staffing requirements, team meetings.	Destroy- 5 years after closure	
PRESS/COMMUNICATIONS		
Events organisation, press cuttings, correspondence with the press, website development.	Destroy- 5 years after closure	
Communications strategy and planning documents, press releases.	Destroy- 10 years after closure	

TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED	PROTECT
Lead directly to widespread loss of life	**Seriously**[2] prejudice public order or individual security or liberty	Prejudice individual security or liberty	Cause **substantial**[2] distress to individuals	Cause distress to individuals
Cause severe long term damage to the UK economy	Threaten life directly	Shut down or otherwise substantially disrupt national operations	Breach proper undertakings to maintain the confidence of information provided by third parties	Breach proper undertakings to maintain the confidence of information provided by third parties
Threaten directly the internal stability of the UK or friendly countries	Raise international tension	Undermine substantially the financial viability of major organisations	Breach statutory restrictions on the disclosure of information	Breach statutory restrictions on the disclosure of information
Cause **exceptionally grave**[2] damage to effectiveness of security of UK, allied forces or intelligence agencies	Cause **substantial**[2] material damage to national finances or economic or commercial interest	Work substantially against national finance or economic and commercial interest	Disadvantage government in commercial or policy negotiations with others	Disadvantage government in commercial or policy negotiations with others
	Seriously[2] damage relations with friendly governments	**Impede**[2] the investigation or facilitate the commission of serious crime	Cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies	Cause financial loss or loss of earning potential or to, facilitate improper gain or advantage for individuals or companies
	Cause **serious**[2] damage to the operational effectiveness of security of UK, allied forces or intelligence operations	**Materially**[2] damage diplomatic relations	Prejudice the investigation or facilitate the commission of crime	Prejudice the investigation or facilitate the commission of crime
		Seriously impede[2] the development or operation of major government policies	Adversely affect diplomatic relations [1]	
		Cause damage [2] to the operational effectiveness of security to UK, allied forces or intelligence	Impede the effective development or operation of government policies [1]	
			Make it more difficult to maintain the operational effectiveness or security of UK or allied forces[1] Undermine the proper management of the public sector and its operations[1]	

Key: [1]Main differences between PROTECT & RESTRICTED [2]**Key differences between levels of Protective Marking**

In addition to a protective marking, a "descriptor" can be used to identify the nature of the information, e.g. CONFIDENTIAL – BUDGET or RESTRICTED – STAFF. Only the descriptor PERSONAL may be used alone.

DESCRIPTOR	Appropriate to use when:
APPOINTMENTS	Actual or potential appointments not yet announced
BUDGET	Proposed or actual measures for the budget before they are announced
CONTRACTS	Tenders under consideration and the terms of tenders accepted
MANAGEMENT	Policy and planning affecting groups of staff
MEDICAL	Reports, records and material relating to individuals
PERSONAL	Material only to be seen by the person to whom it is addressed
POLICY	New or changed SCJC or government policy before publication
STAFF	Contains references to named or staff or personal confidences by staff to management
VISITS	Advance details of visits (e.g. Ministerial; Board members; senior staff)