

Records Management Policy

Cafcass policies are designed to safeguard children, families, carers, staff, and the reputation of Cafcass. They derive from legislation and from what we learn from practice quality audits, significant incidents and learning reviews, feedback, and complaints. They set out what must be done. They are public documents against which we can be held accountable. If they are not adhered to, we can be subject to challenge through complaints, the Parliamentary & Health Services Ombudsman, Social Work England, or even a Judicial Review. A decision not to adhere to a policy must be supported by a compelling rationale and endorsed by a manager. Policies are, therefore, subject to monitoring for compliance – with fair and reasonable consequences for non-compliance. Key policies that are new or updated are subject to attestation by all staff or groups of staff where appropriate.

What is this policy for?

This policy sets out the requirements for the management of Cafcass records, regardless of format or storage location, and is to be read in conjunction with the Information Assurance Policy. It sets out the framework for the ChildFirst Recording and Retention Policy which documents the expected records management procedures for our main information asset, children's records stored in ChildFirst.

Who does it apply to?

This policy applies to all staff, including Cafcass Associates, as all staff create, access, and manage records as part of their daily work. Information Asset Owners have specific responsibilities in relation to the assets they own. Annex 1 lists Cafcass' key information assets and the responsible Information Asset Owners.

Why is this important for children?

Cafcass produces records that concern the lives of children and their families. These records are incredibly valuable as they can help children and their families understand what happened in their family court proceedings and how their unique needs, and their family circumstances, were taken into consideration in Cafcass' recommendations to court. Cafcass must ensure that these records are properly managed, so they can be accessed when requested in line with individual rights under Data Protection legislation, while also protecting sensitive personal information. Doing this consistently is part of Cafcass' commitment to ensure that every child has an exceptional experience of Cafcass.

1. What is records management?

- 1.1 Records management is the control of an organisation's records, from creation to disposal, and is done to meet business needs, statutory and fiscal requirements, and user expectations.
- 1.2 The fundamental principle of records management is to ensure that information is available when and where it is needed, in an organised and efficient manner, and in a well-maintained environment. This means having a detailed catalogue of the paper records we hold, as well as a clear folder structure for the digital records we store in SharePoint and other systems.

- 1.3 Cafcass staff must be aware of the records their team creates, receives, and uses, and these records must be saved in a secure and accessible location, in line with the guidance on where to save a file, which is available on Connect.

2. What is a record?

- 2.1 Records are information that provide evidence of the organisation, its functions, the activities it carries out, and the decisions it makes. Records produced by Cafcass demonstrate how decisions are made by the organisation, how money is spent, and include individual case work, HR files, policy changes, contracts, and projects. Our records not only have evidential value but are of significant emotional value to the children and families with whom we work, who can request access to their records.
- 2.2 Any information which does not have evidential value is not a record and so can be destroyed when it is no longer required.
- 2.3 All records produced by Cafcass must be authentic, reliable, usable and have integrity:

Description	Definition	To meet this standard:
Authentic	An authentic record is a record that is credible and authoritative and could be used as evidence.	Staff must control the creation, receipt, transmission, maintenance, and disposal of records in accordance with the national policies and procedures. Record creators must be identifiable on the records. Cafcass records must be protected from unauthorised addition, deletion, alteration, use and concealment.
Reliable	A reliable record contains content that can be trusted as a full and accurate representation of the transactions, activities, or facts they concern.	Records must be created at the time of the transaction or activity or soon afterwards. They must be created by staff who have direct responsibility for record creation.
Integrity	The integrity of a record refers to it being complete and unaltered.	Teams must have access controls in place to specify what additions / alterations can be made and by whom. Any changes to a record must be clearly indicated by the member of staff making the change. In the case of digital records, this will be automatically logged through version control. All staff are responsible for keeping records secure and for holding them in a format that remains usable until the date of destruction.
Useable	A useable record is one that can be located, retrieved, presented, and interpreted.	It is essential that Cafcass filing systems for both paper and digital records are simple and easily understood by the users of the system.

- 2.4 Cafcass records must not be processed on publicly accessible Artificial Intelligence services. Uploading Cafcass records onto these services would result in Cafcass losing ownership of the record, and therefore not being able to guarantee its authenticity, reliability, or integrity.

3. Who is responsible for our records?

- 3.1 All staff have a responsibility to manage records in line with this policy and to ensure that records are not deleted or destroyed before they reach the end of their retention period.
- 3.2 The National Records Manager is responsible for providing guidance and advice on how to manage records in line with this policy, for developing processes and procedures to improve the management of records and ensuring that all staff are aware of their responsibilities.
- 3.3 Information Asset Owners are responsible for knowing what records their areas process and how they are used, for updating the Information Asset Register to ensure that all records that contain personal data are documented, for ensuring their area is compliant with this policy, authorising the destruction of records in line with the [retention schedule](#), and supporting the National Records Manager where required.

4. Records retention

- 4.1 Cafcass needs to retain records so that it can fulfil its statutory and regulatory obligations, provide an exceptional service to children and families, and continue to operate effectively and efficiently.
- 4.2 The retention periods for Cafcass records are set out in the [Cafcass Retention Schedule](#). Some of these retention periods are determined by law, regulation, standards, or best practice. This is clearly indicated in the Justification column of the [Retention Schedule](#). Where there is no legally defined retention period, Information Asset Owners have assessed the requirement for the information to be kept based on business need to determine suitable retention periods.
- 4.3 The [Retention Schedule](#) includes the retention trigger (the event that starts the retention period), the retention period (the length of time the record must be kept), and the disposal action (what will happen to the record at the end of the retention period).
- 4.4 Records must not be deleted or destroyed before they have reached the end of their retention period unless such deletion is in line with a legislative requirement. The National Records Manager must be consulted prior to any such deletions and the decision and deletion will be recorded on an early deletion of records log held by the National Records Manager.
- 4.5 If information, especially personal data, needs to be deleted or destroyed due to a legislative requirement, such as the right to erasure, then the Information Assurance team must be consulted first.
- 4.6 There are circumstances under which records need to be retained for longer than the stated retention period. Examples of this include a pending or actual legal dispute or action, investigation or inquiry, an active request under Data Protection legislation, a change of legislation or regulations, or to support legitimate business needs. The National Records Manager and the Information Assurance team must be consulted if records need to be retained after their retention period has ended. A decision to retain a record longer than the retention period must be made by the Information Asset Owner following consultation with the National

Records Manager and the Information Assurance team and will be recorded on the extended retention log held by the National Records Manager.

5. Using the Retention Schedule

- 5.1 The [Retention Schedule](#) has been organised according to business functions, such as Analytics, Estates, and Finance, so that users can easily locate the records that relate to their work.

6. Updates to the Retention Schedule

- 6.1 The [Retention Schedule](#) is a living document and must be updated to reflect changes in legislation or regulations, changes in business functions, the introduction of new systems, the creation of new types of information, and to update terminology.
- 6.2 If staff become aware of any changes that would require the [Retention Schedule](#) to be updated, including those mentioned above, they must inform the National Records Manager as soon as possible.
- 6.3 Any significant changes will need to be reviewed by the Information Assurance Board (or equivalent forum) and the Policy Reference Group before being approved by the Corporate Management Team.

7. Records Disposal

- 7.1 Records shall be disposed of as close to the disposal date as possible so that:
- It is easier to determine what information Cafcass holds and to find important information.
 - Storage is used more efficiently.
 - Cafcass adheres to all Principles of the General Data Protection Regulations, specifically article 5 which states that personal data shall be kept for no longer than is necessary for the purposes for which it is processed. Cafcass also adheres to the accountability principle which requires organisations to take responsibility for what they do with personal data, and to have the appropriate records or measures in place to demonstrate compliance.
- 7.2 Records must only be destroyed with the authorisation of the relevant Information Asset Owner or through a process which has been approved by the Information Asset Owner in consultation with the National Records Manager. If you are unsure what the process is for your team, please contact your Information Asset Owner (see Annex 1 for a list) or the National Records Manager.
- 7.3 Records must be disposed of securely to prevent unauthorised access to, and later reconstruction or recovery of that information. For paper records, this requires them to be destroyed by the archive storage supplier or to be placed in the confidential waste bins provided in each Cafcass office. For digital records, this means deleting them from all storage locations.
- 7.4 All disposals must be documented to provide evidence of what has been disposed of, when, and who authorised the disposal. This information must be sent to the National Records Manager who will record it in a national central registry. The information required by the National Records Manager is outlined in Annex 2

Policy Owner	Head of Legal Services
Approved by	Corporate Management Team
Approved on	22 nd April 2025
Implemented	25 th June 2025
Version	1
Amended	N/A
Next review	June 2026

Annex 1: Cafcass' key information assets

The table below outlines the key information assets produced by Cafcass and their Information Asset Owner. This does not cover all the records produced by Cafcass, these are listed in the retention schedule. It groups these records into information assets and assigns an Information Asset Owner for each asset.

Information asset	<u>Information Asset Owner</u>
Business analytics	Head of Analytics
Business Services records	Head of Business Services
Corporate Secretariat records	Director of Resources
Children's files	National Director of Operations
Commissioned Services records	Head of National Commissioning
Communications records	Head of Communications
Complaints and correspondence	Head of Complaints and Correspondence
Finance records	Director of Resources
Health and Safety records	National Estates Manager
Human Resources records	Chief People Officer
IT Systems	Chief Information Officer
Legal records	Head of Legal Services
National Improvement Service records	Assistant Director for Performance and Quality Assurance
Policy and Research records	Assistant Director – Policy
Procurement records	Head of Procurement
Public relations records	Head of Communications
Project Management records	Team Leader of Programme Management Office
Strategy records (strategy co-ordination)	Head of National Commissioning

Annex 2: Information required when destroying records

When destroying paper records held in offsite storage, the National Records Manager must be sent the following information:

- Name of the box (usually found in the major description field on IM Connect).
- Box barcode number.
- Was the whole box destroyed?
- If not, provide a brief description of the file(s) destroyed.
- How was the box destroyed? (Placed in an office's confidential waste or destroyed by Iron Mountain).
- Date of destruction.
- If destroyed by Iron Mountain, please supply the certificate of destruction (this will be sent within 6 weeks of the destruction being requested).

When destroying digital records held in SharePoint or other systems, the National Records Manager must be sent the following information:

- Name of the department or team.
- Brief description of the records destroyed (e.g., invoices).
- Covering dates of records destroyed (e.g., April 2013 – March 2014).
- Number of files destroyed.
- Date of destruction.
- Link to SharePoint folder.