Cafcass Information Assurance Policy

Overview of Policy

This policy sets out the requirements relating to the management of information. It applies to all staff that create, access and manage case-related and other records.

1. Introduction

1.1 The Chief Executive (CEO) has overall responsibility for ensuring that information risks are assessed and managed, supported by the Senior Information Risk Owner (SIRO), The National Child Care Policy Manager**.**

1.2 Day-to-day responsibilities are delegated to the Information Asset Owners (IAOs), the Head of Legal and the Information Assurance Officer. All are available to advise on specific information assurance issues.

1.3 The Information Asset Owners for the following key records ('assets') are:

Case and complaints records	National Service Director
HR & health and safety (Accident & Incident) records	Head of Human Resources
Public relations records	Head of Service (Communications)
Finance records	Director of Resources
IT systems	Head of IT

1.4 It is the responsibility of the IAOs to address risks to their assets and provide regular updates to the SIRO. IAOs must know what information Cafcass holds and how it is used, including responding to requests for access and knowing who has access to the asset information.

1.5 It is the responsibility of the Head of Legal to ensure staff are made aware of the legal obligations relating to information assurance that affects them.

1.6 All staff must undertake training in information assurance. All new staff must undertake information assurance training within 6 months of commencing employment.

1.7 All staff are expected to redo the training every three years but will be expected to keep up to date with bulletins and news items on information assurance which relate to any new legislation or guidance on data protection.

1.8 Failure to comply with instructions contained in this policy may amount to misconduct resulting in disciplinary action.

1.9 This policy should be read in conjunction with Cafcass' IT Policy and Procedures.

2. How to meet information management standards

2.1 All information must be kept securely and adhere to the 'data protection principles' set out in Article 5 of the EU 2016/679 General Data Protection Regulation. Information on the process for reporting and handling data breaches is set out in section 3 of this policy.

2.2 All electronic case files can be found on either ECF or ECMS. Locations of archived paper files must be held by the local office in the first instance; where there is subsequent transfer of records between departments / offices and authorized external organisations, the Governance team must be informed in order to keep a central record of file location.

2.3 Emails are subject to Data Protection and Freedom of Information (FOI) legislation and can also form part of a corporate record. Emails could be used as evidence in legal proceedings and may be released to the public in response to a FOI request.

2.4 Whenever an email is sent or received a decision should be made about whether the email needs to be kept as a record. A record is defined as data forming part of a relevant filing system.

2.5 All records must be authentic, reliable, useable and have integrity.

Description	Definition	To meet this standard:
Authentic record	An authentic record is a record that is credible and authoritative, and could be used as evidence.	Each office must implement Cafcass national procedures as set out in the Case Recording Policy and specific business area procedures. 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 record	A reliable record is one whose content 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 should be created by staff who have direct responsibility for record creation.

Integrity of a record	The integrity of a record refers to it being complete and unaltered.	Offices must have access controls in place to specify what additions / alterations can be made and by whom. Any changes to a record should be clearly indicated by the member of staff making the change. All staff are responsible for keeping records secure and for holding them in a format that remains reliable until the date of destruction.
Useable record	A useable record is one that can be located, retrieved, presented and interpreted.	It is essential that Cafcass filing systems in practice are simple and easily understood by the users of the system.

2.6 Individuals have a right to have inaccurate personal data held by Cafcass corrected and requests for data to be rectified can be made verbally or in writing. Under the GPDR, requests for personal data to be corrected must be responded to within one month of receipt. Therefore, it is important that practitioners amend any incorrect personal information, such as contact details or date of birth, of service users as soon as they become aware that it is inaccurate.

2.7 If Cafcass are satisfied that the personal data held is accurate, individuals should be informed that the data will not be amended and the reason for this decision. A note should be added to the case file to show that the information is contested.

3. Data Breaches

3.1 All data security breaches and other breaches of Data Protection legislation must be reported internally. All staff must inform their line manager and the Governance team via the Governance email address when a breach is known or suspected.

3.2 Breaches and suspected breaches must be reported to the Governance team within 48 hours of staff becoming aware of the breach or suspected breach.

3.3 The instructions to be followed when a data breach is known or suspected are on the Data Breaches intranet page.

3.4 The relevant Service Manager or Business Service Manager/Business Services Team Leader must complete a data breach reporting form within 48 hours of the breach and send the form to the Governance team.

3.5 Under the EU 2016/679 General Data Protection Regulation, breaches of personal data must be reported to the relevant supervisory authority where the breach is likely to result in a risk to the rights and freedoms of the individual. Such risks include loss of control over their data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation and emotional distress.

3.6 For Cafcass, the supervisory authority is the ICO and such breaches must be reported to the ICO as soon as possible but this must be within 72 hours of Cafcass becoming aware of the breach, where this is feasible. The information to be included in the notification to the ICO is set out within the ICO's guidance on personal data breaches. The process for notifying the ICO is managed by the Governance team.

3.7 The information which has to be provided to the ICO is detailed and extensive so the individual reporting the breach must provide as much information as possible to Governance about the circumstances and the content of the data which has been lost or disclosed without authority.

3.8 When assessing whether a data breach should be reported to the ICO, the Governance team will consider the level of risk to the individual by taking into account:

- the nature and sensitivity of the information
- the number and identity of unauthorised recipients

3.9 Each incident will be considered individually but the following are examples of how risk is likely to be assessed:

- Limited personal information such as a name and address disclosed in a Welcome Letter to one individual would be considered to be a low risk.
- Sensitive personal information relating to proceedings disclosed to one individual such as a Safeguarding Letter, would be considered to be a medium risk.
- High volumes of sensitive information disclosed to a large number of unauthorised recipients would be considered high risk.

3.10 Breaches which are considered to be either medium or high risk will be reported to the ICO. Apology letters will also be issued to the affected service users.

3.11 High risk breaches will be identified by the Information Assurance Officer who will refer to the Head of Legal in cases which are complex. High risk breaches will be reported by Governance to the relevant Head of Practice, Assistant Director and Information Asset Owner. The Information Asset Owner may escalate the breach to the Information Assurance Board if they feel this is appropriate.

4. Security of information and Cafcass premises

4.1 Cafcass information held in both paper and electronic form must only be accessed by staff who have a legitimate business requirement to view the information. In particular, access to ECMS cases which are not allocated to the individual practitioner or team, while lawful, should not be exploited, and is therefore prohibited unless there is a reason recorded on the case file for this access. National Office staff who require national case access as part of their work do not need to record this on the case file but must only access those cases strictly necessary.

4.2 Cafcass information must not be sent by staff to their own personal email addresses, in particular if the emails contain personal information about service users or other individuals. Cafcass provides all employees with a secure email address and that is the only email address that can be used for Cafcass business.

4.3 Cafcass staff are authorised to send protected information to agencies and service users via email. This information must be sent using Egress Switch software, which is available to all staff through Microsoft Outlook. For the purposes of this policy, 'protected information' refers to confidential information and any personal data from which an individual can be identified.

4.4 In order to minimise the risk of a data breach:

- Before sending protected information to a new email recipient, staff must send a 'verification' email to confirm the correct email address, which is achieved by the intended recipient confirming their identity (template email for service users here).
- Wherever possible, staff must use the 'reply' option when responding to an email, rather than manually typing the email address, to avoid inaccuracies.
- Always check that the address you are using is the correct one and that the contents/attachments are relevant.
- Always check any post to ensure the correct documents are being sent.

4.5 Staff must actively consider the appropriateness of using email to discuss sensitive subjects. All emails may be monitored by Cafcass to ensure correct usage.

4.6 All staff must remove and lock away any papers and files containing personal information when leaving the office at the end of the working day, or for a major part of the day.

4.7 If a practitioner in exceptional circumstances removes any case papers from the office particular care must be taken to ensure their security.

4.8 All filing cabinets and any other storage containing personal data of any kind must be locked overnight.

4.9 Any papers or documents that contain sensitive, personal or confidential information which require disposal e.g. handwritten notes or meeting papers must be disposed of securely by using the confidential waste bins located in offices.

4.10 Cafcass requires all offices, via the Business Service Manager, to:

- Hold a list of all staff that access the building
- Provide temporary identity passes to visitors to the office
- Insist all desks and printers are clear of personal information on a daily basis, and use lockable cabinets to store personal information.
- Complete an induction checklist with new members of staff
- Be protected by an alarm system when the building is not occupied
- Have lockable internal access systems e.g. keypad, swipe cards. Keypad codes

must be changed on a regular basis
- Keep cabinets where there is no public access
- Lock all communications equipment cabinets and locate them away from public access areas
- Use a key safe with a combination lock or digital locking mechanism

4.11 Cafcass requires all staff to:

- Make sure that all keys are locked away in a key safe when not in use
- Inform Business Service Managers when keys or building passes are lost
- Wear ID badges
- Use lockable cabinets to store files containing personal data
- Make sure all personal information is not visible to members of the public; in particular while travelling ensure that no other person can access any protected information if they are using a laptop, reading paper files or speaking on the phone.
- Ensure any printed information is not left at the printer.
- Ensure their desk is clear when leaving the office at the end of the day, or for a major part of the day
- Always check when information is being sent out that it is being sent to the correct and up to date address
- Check that any correspondence does not contain information about other cases

5. Archiving and record retention

5.1 The retention schedule document (Appendix 1) sets out how long non-case records must be retained. The Case Recording and Retention Policy covers the retention of case records. Records must be archived in accordance with the retention periods document.

5.2 It is the responsibility of all Cafcass staff involved in record management to keep robust management systems in order to retrieve archived records.

5.3 A record should be kept of what records have been destroyed, with a note of authorisation and the method of destruction appropriate to the sensitivity of the record.

5.4 Please seek advice from the Governance Team or IT Security Officer on how to dispose of records that cannot be deleted or shredded.

Appendix 1: **Retention Schedule**

Owned by	Melanie Carew, Head of Legal Services
Approved on	September 2018
Implemented	September 2018
Version	4.7
Amended	Data breach section updated. Process for escalation of high risk breaches and risk assessment criteria added to the policy. Clarification given on the process for handling data breaches.
Next Review	September 2019