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 records ('assets') are:

Case and complaints records	National Service Director
HR and health and safety records	Director 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.

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

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 the Data Protection Act 1998.

2.2 All data security breaches and other breaches of the Data Protection Act must be reported internally. All staff must inform their line manager and the Governance team via the governance email address when a breach is suspected. Cafcass has chosen to adhere to the Information Commissioner's Office (ICO) guidance when a suspected breach occurs which sets out steps to take in order to manage a data security breach. Some breaches may fall within the criteria for reporting to the ICO which is set out within the notification of data security breaches to the ICO guidance. This process is managed by the Governance team.

2.3 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.

2.4 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.

2.5 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.

2.6 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	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

	complete and unaltered.	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.

3. Security of information and Cafcass premises

3.1 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.

3.2 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.

3.3 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.

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

- Protected information (as defined above) must not be sent via fax.
- 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.

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

3.6 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.

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

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

3.9 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

3.10 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

4. Archiving and record retention

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

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

4.3 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.

4.4 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 Periods

Owned by	Melanie Carew, Head of Legal Services
Approved on	July 2017
Implemented	July 2017
Version	4.3
Amended	Reference to Office Managers removed. Asset Owner for HR records corrected.
Next Review	September 2017