Information Assurance 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 things that all staff employed or contracted by Cafcass have to do to manage information securely. Non-compliance leads to challenges and consequences, while exemptions require managerial approval. The policy is monitored for adherence and in addition requires attestation by any individual employed or contracting with Cafcass. The fundamental objective is to protect the integrity of information, safeguard the information of children, families and staff, and maintain accountability within Cafcass in accordance with legislation and the standards of government.

Why is this important for children?

It is critically important that the information we hold on children, which is recognised in law as sensitive, is protected in accordance with all relevant legislation. This policy makes clear the commitment that you make so that you are doing all you can, and what you need to do to ensure this happens. You are a privileged custodian of highly sensitive and personal information which is key to the safety and the futures of children and their families and is also essential for them to understand what happened during Cafcass involvement in their lives. This privilege comes with your responsibilities which are explained in this policy. The impact of sharing information without proper consideration and care will cause harm to children, their families and carers. In some cases, the impact will be irreversible and long lasting. The same is true for information belonging and pertaining to Cafcass colleagues.

1. Introduction

1.1 The Chief Executive Officer has overall responsibility for assurance that information risks are assessed and managed, supported by the Senior Information Risk Owner[1] (the Director of Resources and Deputy Chief Executive Officer) and Deputy Senior Information Risk Owner (the Chief Information Officer).

1.2 Day-to-day responsibilities are delegated to Information Asset Owners[2], the Head of Legal and the Data Protection Officer[3]. All are available to advise on specific information assurance issues.

1.3 The Data Protection Officer at Cafcass is responsible for monitoring internal compliance, advising on our data protection obligations, providing advice regarding Data Protection Impact Assessments and data sharing, and acts as a contact point for data subjects and the Information Commissioner's Office.

1.4 The Cafcass Records Management policy contains a list of Information Asset Owners who, through awareness of the records handled in their respective areas and their applications, are responsible for the lawful management of those records.

1.5 Information Asset Owners, with the support of their deputies and the information Assurance team, must know what information Cafcass holds and how information is used/processed, including responding to requests for access to information and knowing who has access to the asset information. It is the responsibility of the Information Asset Owners to identify and address risks to their assets and provide updates to the Senior Information Risk Owner every 6 months, through the National Records Manager for reporting to the Resources Directorate Management Team meeting (sitting as the Information Assurance Board).

1.6 Staff are made aware of the legal obligations relating to information assurance that affect them by being required to attest that they have read and understood this policy and must undertake regular mandated training on those obligations (see 1.7 and 1.8).

1.7 All staff must undertake training on information assurance. All new staff are required to read this Information Assurance Policy and complete the mandatory 'Protecting Information at Cafcass' e-learning module as specified in their induction programme. Both these requirements must be met before a member of staff can process personal information on Cafcass systems. Specifically, this means that children's cases cannot be allocated to a Family Court Adviser or manager until they have completed both these tasks.

1.8 All staff are required to recertify every three years and are 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.

1.9 Failure to comply with instructions contained in this policy may amount to misconduct

[1] See Appendix A for role of Senior Information Risk Owner
[2] See Appendix B for role of Information Asset Owners
[3] See Appendix C for role of Data Protection Officer

resulting in disciplinary action.

1.10 This policy should be read in conjunction with Cafcass' IT Policy and Procedures. All staff must ensure their use and management of information is compliant with our IT Policy and Procedures.

1.11 In compliance with Cafcass' agreement with the National Police Chief's Council, staff are not permitted to take their work devices (laptop/mobile phones) outside of the UK as this constitutes a cross-border transfer of police data. Where staff are required to attend proceedings outside of the UK, approval has to be sought from their line manager and a request must be submitted in line with Cafcass' IT Policy and Procedures.

2. Requirements relating to records management

2.1 All information must be kept securely and adhere to the data protection principles set out in the Data Protection Act 2018. Information on the process for reporting and handling data breaches is set out in section 5 of this policy. All recorded information is subject to Data Protection and Freedom of Information legislation and can also form part of a corporate record. Cafcass cases and other records could be requested by the court or parties to be used as evidence in proceedings or by an individual as part of an individual's rights request.

2.2 Cafcass information may also be released to the public in response to a Freedom of Information request.

2.3 Whenever an email/letter is sent or received a decision must be made about whether it needs to be kept as a record. A record is defined as data forming part of a relevant filing system. Only information that serves a purpose (meaning that it is relevant and necessary) needs to be retained by Cafcass.

2.4 All information stored must be managed in line with the Records Management policy.

2.5 Cafcass processes and uses AI in accordance with our IT policy, ensuring that all AI applications are piloted and assessed based on Cafcass' processing compliance needs to maintain security and compliance. Staff are not permitted to process any personal information relating to staff or children and families on publicly available internet-based artificial intelligence services (examples of which include Chat GTP and Bard) or otherwise use these services without permission. More detail is contained in the IT Policy and Procedures (section 7.4).

3. Requirements relating to data protection rights

3.1 Individuals' rights under UK data protection legislation are detailed in our privacy notice(s).

3.2 Feedback or requests relating to individuals' rights must be responded to within one month. As these rights are not all absolute, they must be assessed on a case-by-case basis. Advice is available from the Information Assurance team and from Connect explaining the different rights. Some requests can be managed locally as part of the

team's day to day activities, but where more complex requests are made, support should be sought from the Information Assurance team.

3.3 Cafcass is required to ensure that all information processed is fair, relevant, accurate and necessary. Where appropriate, a note must be added to the child's case file to make clear if any information has been disputed and by whom, as this ensures we maintain an accurate record of our processing. For further information on the requirements of case recording please refer to the Recording and Retention policy.

4. Requirements relating to security of information and Cafcass premises

4.1 Cafcass information held in either paper or electronic form must only be accessed by staff who have a legitimate business requirement to view the information. Personal information held on ChildFirst, or other Cafcass systems, must only be accessed electronically by those with a legitimate need to be processing the information.

4.2 Access to children's cases on ChildFirst which are not allocated to the individual practitioner or team must be carefully managed, and, while lawful, is prohibited unless there is a clear and explicable business need which should be recorded and agreed. Corporate Services 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 which are strictly necessary for the performance of their duties.

4.3 Cafcass information must not be sent by staff to their own personal email addresses/phones or to other non-Cafcass managed storage (such as Dropbox, Google Drive or personal Microsoft OneDrive); Cafcass-provided devices (mobile phones and laptops) must be the only devices used to process Cafcass data.

4.4 Although information processed by Cafcass Associates is managed through a contractual arrangement in conjunction with the Bring Your Own Device policy between Cafcass and Cafcass Associates as defined in section 6 of the IT Policy and Procedures, Cafcass Associates are also required to attest to having read and understood this policy.

4.5 Cafcass staff send protected information to third parties and children and families via email. This information must be sent using Cafcass encryption 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.

4.6 To minimise the risk of a data breach, everyone must:

- Use the 'reply' option when responding to an email, rather than manually typing the email address, to avoid inaccuracies.
- Where possible, send emails directly from ChildFirst.
- When sending emails containing protected information from a work phone, prefix the subject heading with the word 'encrypt' to ensure the email is sent securely.
- Always check that the post or email address used is the correct one and that the contents/attachments are relevant.
- Always check post to ensure the correct documents are being sent.

4.7 A data breach will occur if directly or indirectly identifiable personal information shared is

not accurate, relevant and necessary to the processing.

4.8 Staff must actively consider the appropriateness of using Cafcass email to discuss sensitive subjects if personal use is made of Cafcass systems, in line with the IT Policy and Procedures. All emails are monitored by Cafcass and may be audited to ensure correct usage.

4.9 If a practitioner, in exceptional circumstances, removes any case papers from the office, they must have sought and gained line management approval and particular care must be taken to ensure their security.

4.10 Cafcass is a digital-first organisation but there may, on occasion, still be personal data stored on paper (however temporarily). This must be secured effectively, and all filing cabinets in offices and any other storage containing personal data of any kind must be locked overnight.

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

4.12 Laptops and iPhones are securely disposed of using ADISA certified organisations. Cafcass also uses Mobile Device Management techniques which allow remote erasure of equipment. Removable media which requires secure disposal can be sent to the IT team. See section 2.21 of the IT Policy and Procedures.

4.13 Cafcass requires all offices, when staffed, 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.
- Check printers for any printing that hasn't been collected when there is cover on site, which for larger sites is usually every day. Printers are not based in areas accessible to children and families.
- 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.

4.14 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 when on Cafcass premises.
- 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.
- Use lockable cabinets to store files containing personal data.
- Make sure 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 using a laptop, make sure the built-in privacy screen is used. When reading paper files ensure you are not overlooked and when speaking on the phone ensure you are in a private space where you cannot be overheard.

- Log out of or lock computers or smartphones when not in use or left unattended, even for short periods.
- Not leave any printed information at the printer.
- Clear desks 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.

4.15 The requirements for Cafcass staff to keep information secure apply across all working environments, including Cafcass offices; staff homes; and during remote/mobile working. Staff working remotely must take particular care to ensure the security of information outside of Cafcass offices by ensuring all information is stored securely away when not used and work-related activity is undertaken in secure/private settings.

5. Requirements relating to data breaches

5.1 All breaches of data protection legislation must be reported internally as described in this section. Staff must immediately inform their line manager or covering manager as soon as a breach is known or suspected and simultaneously alert the Information Assurance team at governance@cafcass.gov.uk.

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

5.3 Breaches and suspected breaches must be reported to the Information Assurance team at governance@cafcass.gov.uk as soon as possible and no later than 24 hours after becoming aware of the breach or suspected breach. This is so that the seriousness of the breach can be assessed, and action taken to mitigate the impact of those effected and keep children, families, and staff safe. This also allows for timely assessment of any need to report the breach further for instance to the Chief Executive Officer, Board or to the Information Commissioner's Office, and/or follow the Significant Incident Response process.

5.4 Breaches that have been assessed as high risk must be notified to Cafcass' core Corporate Management Team (CMT) via the raising of a Serious Incident Response (SIR) which will also notify CMT of the commencement of ICO notification process.

5.5 Notification of high-risk breaches must be made to the UK supervisory authority, the Information Commissioner's Office, within the statutory 72 hours of Cafcass becoming aware of the breach, where this is feasible. 'High risk' in this specific context is defined as a breach likely to result in a risk to the rights and freedoms of individuals. Such risks include threats to physical or emotional safety, loss of control over data or limitation of individual's rights, discrimination, identity theft or fraud, financial loss, damage to reputation or emotional distress.

5.6 The process for notifying the Information Commissioner's Office is managed by Cafcass' Data Protection Officer or their Deputy. The information required by the Information Commissioner's Office is extensive, so those involved in the breach must provide as much information as possible to the Information Assurance team about the circumstances,

context and risk associated with the breach.

5.7 Actions taken and learnings identified will be captured for the SIR and form part of the notification to the Information Commissioners Office.

5.8 When assessing whether a data breach meets the significant threshold for reporting to the Information Commissioner's Office, the Data Protection Officer or their deputy will consider:

- The lawful basis in the processing of information,
- The nature and sensitivity of the information,
- The number and identity of unauthorised recipients,
- The suspected impact/risks to those whose information has been breached,
- The suspected impact/risks on the recipient of the information; and
- The potential impact on Cafcass.

5.9 Each incident will be considered individually, and the Data Protection Officer/ Deputy Data Protection Officer will support and advise the reporting manager in assessing the risk and identifying next steps in the event of a breach or potential breach.

5.10 Apology letters, following confirmed data breach, must be issued to those affected. The Information Assurance team must be consulted and are responsible for supporting the relevant senior manager in ensuring the apology letters reflect the nature of the confirmed breach.

5.11 Breaches that are identified as high risk (see paragraph 5.4) will be raised with the Data Protection Officer, Senior Information Risk Owner, Head of Practice and Head of Legal in the first instance. These breaches will be reported by the Information Assurance team to the relevant Head of Practice/Profession, Assistant Director and Information Asset Owner who will raise a Significant Incident Report which will in turn inform relevant Corporate Management Team members including the Chief Executive Officer.

Policy owner	Head of Legal Services
Approved by	CMT and Policy reference group
Approved on	December 2025
Implemented	19th November 2024
Version	6.1
Amended	November 2024: Records management has been moved to its own new records management policy; change of internal reporting from 48 to 24hrs; addition of roles and responsibility of Senior Information Risk Owner, Information Asset Owners and Data Protection Officer; change in staff needing to read this policy and complete data protecting information at Cafcass e-learning training prior to accessing children and families' records; compliance when taking work devices abroad due to the National Police Chief's Council agreement. November 2025- amendment to 2.5- addition of AI use in accordance with IT policy.
Next review	November 2028

Appendix A:

Role of the Senior Information Risk Owner (SIRO)

Cafcass' Senior Information Risk Owner is the Director of Resources and Deputy Chief Executive, and the Deputy Senior Information Risk Owner is the Chief Information Officer.

The main responsibility of the Senior Information Risk Owner (and their deputy) is to:

- Establish and chair an Information Assurance Board or equivalent forum to oversee the information risk management process and provide assurance to the organisation's Board and Audit and Risk Assurance Committee.
- Ensure Cafcass has designated staff with defined responsibilities including Information Asset Owners who understand their roles and are supported by appropriate information risk and governance policies.
- Ensure Cafcass has a risk awareness and training programme of work that is appropriate.
- Oversee the implementation of policies, standards, and controls for information governance and assurance, and promote a culture of information risk awareness and responsibility across the organisation.
- Act as the central point for information risk management at Cafcass including resolution of any escalated risk issues raised by Information Asset Owners, the Data Protection Officer, auditors etc.
- Develop and maintain an information risk strategy and appropriate policies that set out the organisation's approach to information risk management and which defines the roles and responsibilities of key stakeholders.
- Ensure that information assets are identified and classified according to their value, sensitivity, and criticality, and that appropriate owners and custodians are assigned to them.
- Ensure that information risk assessments are conducted regularly and consistently, and that the results are documented and reported to the relevant stakeholders and authorities.
- Ensure that information risk incidents are reported, investigated, and resolved promptly, and that learnings are shared and acted upon.
- Ensure that information risk awareness and training programmes are delivered to all, and that compliance with information security and privacy policies and standards are assessed and enforced.
- Review and approve any major changes or projects that may have an impact on information risks and ensure that information risk considerations are embedded in the organisation's change management and project management methodologies.
- Keep abreast of the latest developments and best practices in information risk management and ensure that Cafcass adapts and responds to any emerging trends, threats, or opportunities.

The Senior Information Risk Owner will foster a positive and collaborative culture of information risk management across Cafcass and inspire trust and confidence in Cafcass' ability to manage its information risks effectively and efficiently.

Appendix B

Role of the Information Asset Owners (IAO)

Information Asset Owners at Cafcass are usually Heads of Professions. Their role is to understand what information is held within their area, how it is used, who has access to it and why, so that they can understand and address risks to the information. The main responsibilities of Information Asset Owners are to:

- Promote a culture that values and protects information.
- Complete the Protecting information in Cafcass learning and be familiar with all Information Assurance policies and procedures.
- Ensure that any team or area-level plans reinforce this culture of valuing and protecting information.
- Ensure that all information assets in their area are managed in compliance with UK General Data Protection Regulation.
- Ensure that staff have adequate time to carry out information management activities and monitoring so that all information assets are appropriately managed.
- Know what information their area holds.
- Ensure that the Information Asset Register is kept up to date.
- Negotiate, manage and approve data sharing agreements between Cafcass and third parties.
- Ensure their staff follow the Information Assurance policies and procedures for the protection of personal data.
- Know who has access to the information in their area and how it is used.
- Set clear expectations of staff supported by IT access controls to ensure that access provided to information is limited to those with a genuine business need.
- Understand Cafcass' policies on the use of information.
- Ensure that any checks on storage usage and access required are being completed.
- Understand and address the risks to the information they hold and provide assurance to the Senior Information Risk Owner.
- Ensure that appropriate risk assessments such as Data Protection Impact Assessments are carried out. Data Protection Impact Assessments are necessary where processing activities are likely to result in a high risk to the rights and freedoms of individuals.
- Ensure that any risk decisions are taken in accordance with Cafcass' Risk Management Policy and Procedure.
- Take an active role in identifying and reporting new risks.
- Ensure the Data Protection Impact Assessments reflects risks and has been formally signed off by the Senior Information Risk Owner or their deputy, and the relevant Director, where information relating to individuals, or aggregated information, needs to be shared outside Cafcass for purposes other than regular case work.
- Where data based on your information assets is being published or shared externally, ensure the correct level of scrutiny is provided before sign-off.
- Ensure that any requests for information by the Information Assurance team, including the Customer Services team, are responded to in a timely manner.

Information Asset Owners also have specific responsibilities for the management of records in their area, which are outlined in section 3.3 of the Records Management Policy.

Appendix C

Role of the Data Protection Officer (DPO)

The Data Protection Officer (or their deputy) has responsibility to advise on and monitor Cafcass' compliance with the Data Protection Act 2018 and UK General Data Protection Regulation and make recommendations to improve Cafcass practices.

The Data Protection Officer should:

- Act as the main point of contact for data protection issues within the organisation and with external stakeholders, such as the Information Commissioner's Office or data subjects.
- Advise and inform the organisation on its obligations and responsibilities under the relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the Data Protection Act 2018 by monitoring and overseeing Cafcass' compliance with data protection laws and regulations, as well as its own policies and procedures relating to data protection.
- Provide guidance and support to staff on data protection matters, such as data subject rights, data breaches, data sharing, or data retention.
- Ensure that both Cafcass and the data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them.
- Give advice and recommendations to Cafcass about the interpretation or application of the data protection rules and act as a point of escalation for data protection concerns.
- Ensure the creation of a register of processing activities.
- Ensure Cafcass complies with data protection and accountability obligations relating to information assurance.
- Respond to queries from the regulator when it receives complaints about Cafcass' processing.
- Ensure that complaints from data subjects are appropriately escalated and handled.
- Draw Cafcass' attention through the Information Assurance Board (or equivalent forum) to the information risk management process and provide advice to the organisation's Board and Audit Committee of any failure to comply with the applicable data protection rules.
- Develop/advise/monitor completion rates for Information Assurance training.
- Be involved in Data Protection Impact Assessments as required.
- Ensure appropriate auditing of Information Assurance practices is in place by conducting or coordinating regular audits, reviews, or assessments of the organisation's data protection practices and identify any gaps or risks that need to be addressed.
- Report any data protection issues, incidents, or breaches to the relevant authorities and stakeholders, and implement corrective actions or improvement plans as necessary.
- Keep abreast of the latest developments and best practices in data protection and update the organisation's policies and procedures accordingly.