IT Policy and Procedures

Cafcass policies are designed to safeguard children, families, 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?

IT plays a crucial role in service delivery at Cafcass. For that reason, Cafcass staff, permanent, temporary and consultant, must meet and maintain a standard of use in accessing all relevant systems and data. This policy outlines these standards of use.

Who does it apply to?

This policy and associated procedures apply to Cafcass staff and all other parties who are given access to Cafcass digital information, devices and premises, including but not limited to technology providers, Associate FCAs, researchers, Board members, other contractors and agents.

When individuals access a Cafcass provided laptop or phone or use a Cafcass system, they automatically accept the terms outlined in this document.

Why is this important for children?

Cafcass has a duty to support staff to work effectively and securely and to safeguard all personal data and information pertaining to children and families. To that end, this policy clearly sets out procedures and requirements for the provision and management of IT equipment, hardware and software. By adhering to this policy we are able to strike the right balance between protecting information and enabling the provision of our best possible service to children and families.

Policy owner	Chief Information Officer
Approved by	CMT
Approved on	01-Apr-2025
Implemented	01-Apr-2025
Version	7.0
Amended	13-Mar-2025 7.0- Simplification of language. Reflection of new external cyber security assessment regime. Strengthening of section on AI.
Next review	March 2026 (or by projects)

Contents

1.0 Policy statement

1.1 Cafcass depends on secure and reliable technology to deliver its services. The technology is supported by well-trained staff to ensure a high level of service delivery. Maintaining IT systems in good working order is crucial as services to children and families depend upon accurate, timely and safe transfers of data and information.

1.2 Cafcass operates a risk management framework (RMF) which monitors and controls the confidentiality, integrity and availability of all IT systems. The RMF:

a) Makes assessments of the potential threats, vulnerabilities and associated controls to reduce risks to people, information and infrastructure to an acceptable level. This supports compliance with relevant statutory obligations and protections and is guided by the Government Security Policy Framework and associated publications. Assessments are made at organisational, Information Asset Owner (IAO) and system levels, taking into account the probability and impact of a risk materialising.

b) Only permits the deployment of systems that are engineered to meet the requirements for acceptable residual risks defined at each of the assessment levels (organisational, IAO and system). Compliance is monitored continuously. Cafcass:
- Identifies its current cyber security risks and manage its response to them;
- Protects IT resources from known exploits using electronic and procedural controls;
- Monitors the use of its resources so that it is aware of any failure, attack or imminent threat;
- Responds to failures, attacks or imminent threats at sufficient speed to minimise damage, gather evidence for prosecution and alert authorities; and
- Has in place recovery procedures to reinstate services that have failed.

c) Maintains staff awareness of the potential vulnerabilities of systems via various communication channels (for example, email cascades, simulation exercises and intranet bulletins) to ensure staff are aware of the importance of procedures and of regular training. Cyber security training is a mandatory requirement for Cafcass staff.

1.3 Cafcass will normally use IT services provided by external suppliers. It will engage with suppliers throughout the system lifecycle to ensure Cafcass' risk management requirements are met by all members of staff and others including supplier staff and subcontractors. Others with access to Cafcass' information and facilities must do the same.

1.4 In cases where Cafcass develops its own systems, the RMF will be adhered to throughout the development lifecycle, ensuring that our risk management requirements are met throughout the whole development process.

1.5 The procedures outlined in this document describe the principles for the allocation and secure use of IT equipment and facilities. All steps to maintain the integrity of data and systems and to reduce risk are deemed to be accepted and understood by all those accessing and/or taking receipt of any equipment that allows access to Cafcass' network, systems or other facilities.

2.0 Security procedures

This section explains how all those who are given access to Cafcass devices and applications must contribute to maintaining the security of Cafcass' electronic information.

2.1 All Cafcass staff and system users are responsible for contributing to the security of information systems and data belonging to Cafcass. They are also responsible for reporting breaches of this policy to their managers and other appropriate staff members immediately (see 2.7 below).

2.2 Cafcass will treat violations, repetitive breaches, or behaviour which is clearly illegal or offensive or in breach of policy, or which may put Cafcass' reputation at risk, as a disciplinary matter.

2.3 Auditing may be implemented on all systems to record login attempts and failures, successful logins and changes made to all systems, however accessed. Cafcass has the right, if it so wishes, to access any material sent or received by employees using the Cafcass network. Internet usage will be fully monitored and emails will be scanned for content but not routinely manually monitored. Also refer to sections 4.1 and 4.4 which explain that the same is in place for mobile phone use.

2.4 Cafcass reserves the right to override any applicable passwords for the purposes of retrieving and accessing information or files maintained in or on the organisation's property or transmitted through or stored on the organisation's systems, email or other technical resource at any time, regardless of how they have been named, without the permission of the employee and without notice.

Requirements

2.5 Equipment, internet access (including wireless broadband) and email access provided by Cafcass is intended for Cafcass business use, but limited access for reasonable personal use is allowed[1]. Unusual usage will be highlighted to budget holders/managers. This is a high trust model subject to continuous review for compliance.

2.6 Cafcass business **must not** be transacted on personal devices or on devices belonging to other organisations except where the criteria described in table 3.2 is met.

2.7 All those to whom this policy applies must:

a) Ensure all use is compliant with the Information Assurance policy;

b) Complete all training appropriate for your role;

c) Follow the system-enforced parameters for password length and complexity on all devices issued and systems accessed and any other guidance that may be issued;

d) Not share usernames or passwords, or write these down, or access any device with any credentials other than your own;

[1] This might include, for example, occasional limited personal use of the internet where this does not incur data costs nor interfere with delivery of Cafcass duties.

e) Use different passwords for different services (do not reuse the same password or PIN);

f) Change passwords immediately if you suspect that someone else may have had access to them;

g) Not use Cafcass' time, facilities, equipment or supplies for a private business;

h) Not use any personal (or other non-Cafcass) IT equipment together with any Cafcass IT equipment (including Cafcass smartphones and SIMs) with the specific exceptions noted here[2]. Under no circumstances should any personal equipment be used to circumvent the Information Assurance policy or otherwise store, process or transfer Cafcass data. See section 2.15 for more information on the use of removable media;

i) Ensure all use of mobile telephones, including smartphones, is consistent with section 4 of this document;

j) Ensure that Cafcass IT equipment is stored safely and out of sight when not in use, both in and out of the office;

k) Always lock your laptop when you are not using it (press the Windows logo key + L key at the same time) and when you are using your laptop in public always use the built-in privacy screen to protect the information on your screen;

l) Log out of or lock your computer or smartphone when not in use or left unattended, even for short periods;

m) Ensure all internet use complies with Cafcass guidance, including the training module on the use of social media and the Social Media policy;

n) Ensure all email use complies with Cafcass guidance, this includes not auto-forwarding emails to non-Cafcass accounts;

o) Avoid password-protecting documents. If a password-protected document is required the password must be known by more than one person at all times so that the information can be retrieved;

p) Immediately report all IT equipment[3] thefts and losses to:
   - The Littlefish service desk (Tel: 03303 903 703)
   - Your manager
   - The Cafcass information assurance team

[2] Exceptions are where the non-Cafcass equipment is plug and play (that is, where there is no requirement for a third party driver to be installed), which can include: printers, mice, screens and keyboards; VGA, DVI, DisplayPort and HDMI screens and projectors; mobile phones and other devices for charging purposes only; Bluetooth or wired headsets, speakers and microphones for phone or laptop, cars for mobile phones. Under no circumstances does Cafcass guarantee any personal peripheral will function and Cafcass will not be held liable for any damage caused by its use with Cafcass equipment

[3] 'IT equipment' includes but is not limited to laptops, tablets, smartphones, mobile phones, USB data sticks, SIM cards and optical disks.

q) Immediately report all breaches of this policy to:
   - The Cafcass information assurance team
   - The Cafcass IT team
   - Your manager

r) Keep all doors to comms rooms and cabinets locked and secured and ensure locally-documented procedures cover access controls;

s) Supervise at all times all contractors working within comms rooms;

t) Ensure general office security addresses the physical security of all IT equipment;

u) Note that while permissions to systems are granted in proportion to the business need, some systems are locked down by default and may require a registration or approval process. If your role requires any access to systems that was not granted by default, locate and follow the relevant process on the intranet or ask the Cafcass IT Team for guidance;

v) Return all IT equipment when leaving Cafcass' employment, and do not use Cafcass IT equipment or systems after any official leaving date. Exceptions may be granted by the line manager in specific cases, such as sessional workers completing casework after their employment contract end date;

w) Take responsibility for ensuring that you regularly shut down and power off (not sleeping or hibernating) your laptop on at least a weekly basis, in order that important security patches may be applied. If your laptop has not connected to the network for more than two weeks (either via the internet or in a Cafcass office), you must ensure that when you next connect, you do so for a period of two hours to enable your device to catch up with any missing updates; and

x) Beware of social engineering techniques that will attempt to lure you into inadvertently infecting your system with malicious content or into compromising sensitive data. Never click on any links contained within suspicious or unsolicited emails, and report anything suspicious to the Littlefish service desk. Information about phishing emails can be found on the phishing awareness page on Connect.

2.8 Any member of staff with administrative level access to key systems (such as, Microsoft 365 services, Azure, the Cafcass intranet or the Cafcass case management system), which allows them to grant or elevate others' access rights, will be required to go through additional vetting to obtain Security Clearance (SC) before unsupervised access is granted.

2.9 A staff member's standard account for a system must have no administrative privileges. Separate accounts for administrative purposes must be provided. Where a system is capable of multi-factor authentication it must be implemented and used for all accounts.

Working overseas

2.10 All staff must obtain permission from their manager and then complete the "International Travel" service request on the Littlefish Portal before taking any Cafcass equipment abroad (including smartphones) or before accessing Cafcass data from outside the UK. Visiting some countries, even while simply carrying a Cafcass phone, could expose us to a risk of a data breach and may increase your personal risk. You are advised to raise your request in plenty of time before you intend to travel, as some countries may take longer to approve than others. Make sure you list all the countries you will be visiting, even if you are just transiting through or temporarily stopping off, and not necessarily planning to work there. Automatic alerts are generated when devices are used abroad, so should you fail to act in advance your account is likely to be temporarily disabled. Please note that the act of switching on your phone, even if only to make a telephone call, nevertheless constitutes accessing Cafcass data.

2.11 In response to your request, you may be sent guidance about working abroad which you must review. You should also ensure a voicemail PIN is set up for your iPhone before you leave and read the Foreign Commonwealth and Development Office overseas guidance published on the internet for each and every country you plan to visit, including those through which you may simply be transiting[4].

Passwords

Passwords are required to ensure that Cafcass devices and systems are only used by authorised staff.

2.12 Laptops:

a. Laptops are secured using BitLocker and Windows Hello for Business.

b. BitLocker requires the correct PIN to be entered on each laptop start-up.

c. Windows Hello for Business secures laptops by enabling authentication in four possible ways:
   i. Password.
   ii. PIN.
   iii. Fingerprint recognition; and
   iv. Facial recognition.

   The BitLocker PIN and Windows Hello for Business PIN must not be the same.

d. All four methods of authentication may be set up in Windows Hello for Business (the password is required in all cases) but only one is needed at any one time to gain access to a Cafcass laptop.

[4] Data tariffs for international roaming, especially outside the EU and on boats and planes, can be very high (and may be uncapped); check our current mobile network provider guidance for more information. Where possible, Wi-Fi should be used. Switch off data roaming before you leave the UK, otherwise your phone will automatically seek out an internet connection when you reach your destination and you may start using data without realising it.

2.13 iPhones:

a. iPhones are secured using Apple's iPhone encryption. This uses a six-digit PIN and fingerprint or facial recognition.

b. iPhone encryption must be set up on receipt of a phone. A mandatory PIN and optional fingerprint recognition or facial recognition can be set up but only one of these is required to gain access to a Cafcass iPhone.

2.14 Systems:

a. There is a requirement for Cafcass and all its suppliers to hold Cyber Essentials or equivalent as a minimum security accreditation. In order to gain Cyber Essentials, rules for passwords are specified.

b. System passwords must be set up and maintained in line with supplier requirements. These may vary between systems but all will meet the minimum requirements of Cyber Essentials and Cafcass security.

Removable Media

2.15 Removable media includes all types of digital storage which are not physically fixed inside a computer and includes the following:

- Memory cards (like those used in cameras)
- USB pen drives
- Removable or external hard disk drives (HDD) or solid state drives (SSD)
- Mobile devices (iPod, iPhone, iPad, MP3 player, other mobile phones)
- Optical disks (e.g. DVD and CD)
- Floppy disks
- Backup tapes.

2.16 The use of removable media is not prohibited at Cafcass but alternatives should be used wherever practicable.

2.17 Removable media may only be used where there is an identified business need.

2.18 Removable media provided to Cafcass staff to obtain work-related documents or other material such as video can be **viewed** and accessed on Cafcass laptops. If you have any technical questions or security concerns about accessing external media please contact the service desk. Data can be transferred from these third-party supplied media to your laptop if it is necessary for work purposes.

2.19 The transfer of Cafcass information to removable media is only permitted when the removable media is correctly encrypted and there is no practicable alternative. When using removable media, a USB device should be used. USB devices will be automatically encrypted when plugged in to a Cafcass laptop using BitLocker. Once the USB device is encrypted information can be added to it. When using a USB device to hold Cafcass information, under no circumstances should the password for the device be stored or transported with the USB device. This is so that the information on the USB device can only be used by the person intended to use it. It is advisable to seek manager approval before taking this approach to sharing information and a record should be kept on the case file.

2.20 Removable media must be physically protected against loss, damage, abuse or misuse when in use, storage and transit.

2.21 Removable media that has become damaged should be kept securely in a local office with other IT equipment disposals and added to the next collection for secure disposal to avoid data leakage. Contact the IT Team to arrange collection.

2.22 When the business purpose has been satisfied, the contents of the removable media should be deleted from the removable media through a destruction method that makes recovery of the data impossible. Alternatively, the removable media and its data should be destroyed and disposed of beyond its potential reuse. Advice on how to do this can be gained from the Cafcass IT Team.

3.0 IT Allocation Procedures

This section clarifies the allocation rules for Cafcass IT equipment, user accounts and those services funded by local or corporate budgets. Each Cafcass employee is issued with a standard bundle of IT equipment.

Allocation rules for standard IT equipment

3.1 The table below outlines the allocation of standard IT equipment in relation to the job role. There is no charge to budget holders for standard IT equipment, provided that overall volumes do not increase above the volume used to set the annual IT budget.

3.2 Each member of staff should only have one laptop and one phone at any given time unless there are exceptional circumstances. Once allocated, the swapping of device types is not permitted unless supported by an Access to Work or Occupational Health Assessment, or where local or corporate budgets cover the procurement of an additional or alternative device.

Staff groups	Equipment
• Associate Family Court Advisers and Ofsted Inspectors	• Account for online services only • All email is encrypted using Egress by default • No hardware is provided – bring your own device (BYOD) is enabled (see section 6)
• Business Services • Family Court Advisers • Student Social Workers • NQSWs (including those on 100-day placements)	• Touch screen laptop • Apple iPhone The precise model provided will be subject to availability depending on stock levels at the time.
• All other staff including Bank Workers, CMT, OMT and corporate staff	• Touch screen laptop • Apple iPhone or voice only phone or voice with data phone The precise models provided will be subject to availability depending on stock levels at the time.
• Corporate suppliers, researchers and consultants	Equipment and accounts for representatives of our suppliers will be granted on a case-by-case basis. This may include either hardware or online access.
• Improving Child and Family Arrangements (ICFA) provider staff	Access to the ICFA portal only (multi-factor authentication (MFA) is required).

Note: There is a three working-day lead time service level agreement to provide equipment for new starters but five days are recommended to ensure all approvals are completed.

Note: All access is subject to confirmation that relevant security clearances (e.g. DBS check, SC) and technical requirements (for BYOD) are in place.

3.3 Where local or corporate teams or individuals require different or additional equipment (e.g., screens but **not** mice or keyboards) to that specified under the allocation rules for a particular role, this will need to be approved by the IT team via a service request with the cost of the equipment funded by that local or corporate area. Mice and keyboards are the exception and must be ordered through local arrangements.

3.4 Where local or corporate teams require additional equipment for staff not accounted for in the IT budget at the beginning of the financial year (such as an additional post or staff employed for a specific project), this will need to be approved by the IT team with the cost of the equipment and user account funded by the local or corporate area.

3.5 Laptops are not provided with mobile broadband capability. They must connect to Cafcass systems either by wired connection or WiFi. Connecting to Cafcass office WiFi and to GovWiFi is designed to be automatic.

Other IT equipment

Mobile phones (iPhones and voice only)

3.6 iPhones are provided as standard equipment, the provision of which is managed by Littlefish. Newly-issued iPhones are supplied with a headset, charging cable, case and screen protector.

3.7 Additional/replacement iPhone accessories such as protective cases, screen protectors, headsets and charging cables should be ordered locally with the costs covered by the local or corporate area.

Particular needs hardware and software

3.8 Specialist hardware and software (e.g., keyboards, Dragon software) are available to individuals with particular needs. These will be identified by recommendations within formal Access to Work or Occupational Health assessments and subsequently agreed by the HR and IT teams as reasonable adjustments. This and other specialist office equipment can be ordered via a Particular Needs Service Request and is paid for out of local or corporate budgets.

Equipment returns

3.9 Any equipment including laptops, iPhones and voice only phones not actively being used by staff must be returned immediately by completing a Return Equipment service request, otherwise additional costs will be incurred. If the equipment has been swapped as part of a fault/break fix request, the faulty kit will be collected as part of the replacement process.

3.10 Equipment (laptops, iPhones, voice only phones and their peripherals) for those on extended periods of absence must be returned unless a specific local agreement is made with an individual to support 'keeping in touch' arrangements. Managers are responsible for completing a 'User Account – Suspend' request which will incorporate the account suspensions and equipment returns. Accounts will be restored and equipment reallocated to such staff upon their return to work, noting there is a minimum three working day lead time for fulfilment of the 'User Account – Return to Work' service request. Accounts will not be deleted whilst suspended for these purposes and no data will be lost. The hardware allocated on return to work will be in line with the allocation policy and equipment in use at that point in time.

3.11 On leaving Cafcass, the individual's manager is responsible for arranging account deletion and equipment return via a 'User Account – Delete' service request. Requests should be submitted a minimum of 5 working days prior to the leave date, where possible. Local or corporate budget centres will be charged if the issued equipment is not returned at the point of staff leaving or where equipment is damaged and replacement equipment is required. Line managers will be informed of the loss of or damage to IT equipment.

Equipment not to be returned to Littlefish

3.12 Do not return:

- Working keyboards or mice – these should remain on site;
- Rucksacks – these should be returned to the local office and reallocated to new starters; or
- Used phone headsets (ear bud type) – these are to be disposed of and not reallocated.

4.0 Mobile Phone Procedures

This section sets out the procedures for the use of corporate mobile phones (both iPhones and voice-only) in Cafcass and is deemed to have been accepted on receipt of a phone.

Usage

4.1 Line managers are accountable for monitoring the responsible use of iPhones and mobile phones (both voice and data usage) and for taking appropriate action in the event of misuse. In-depth call reports can be requested from the IT team, who will also conduct regular audits of usage and highlight unusual patterns of use.

4.2 Each employee is responsible for all calls and data usage on their iPhone or mobile phone provided, and therefore should not loan or transfer these to anyone else nor allow unauthorised wireless connections that give non-Cafcass staff or devices access to its services (a password must be set to allow access to the hotspot function).

4.3 The dissemination of mobile phone numbers should not be restricted. All employees should include their mobile number in email signatures.

4.4 Cafcass has a 4GB monthly mobile data allowance per device. Allowances are pooled across the organisation. Data is reviewed regularly and increased as required. Individual use is routinely monitored. Managers will be informed if there is a pattern of high or unusual usage of data, calls or text messages.

4.5 Unless there are exceptional circumstances, a Cafcass mobile number will not be transferred to another provider when a staff member leaves the organisation. If a PAC (porting authorisation code) is issued there may be charges levied to cover administration and the remaining term of the contract.

4.6 Staff must fully reimburse Cafcass for the cost of all private voice and text messages and data usage made on company mobile devices where such costs are incurred.

4.7 Loss, faults or damage to all phones should be reported to the Littlefish service desk immediately.

Mobile phones and driving

4.8 It is illegal to use a handheld mobile device when driving. Cafcass does not permit staff to use handheld mobile phones or iPhones when driving.

4.9 It is not illegal to use a hands-free mobile phone or iPhone whilst driving a vehicle. However, if doing so you must ensure you remain able to drive safely with due care and attention and remain in control of the vehicle in accordance with road traffic legislation as outlined in the Highway Code.

4.10 Cafcass staff are not required to use hands-free technology when driving. Any member of staff who wishes or chooses to do so should keep the call to a short duration, ensure that they remain able to drive safely with due care and attention, remain in control of their vehicle and arrange to continue the call when they are no longer driving, and it is safe to do so. Otherwise, they should not accept any call when driving.

Security

4.11 Staff using iPhones:

a) Must complete the full set-up as per the guidance using both:
- A PIN, fingerprint or facial recognition to access the iPhone (only one will be required each time the phone is unlocked after setup); and
- A password to secure the hotspot.

b) Should note that only apps available in the Comp Portal store will be permitted on Cafcass iPhones.

c) Must not use the messaging features of apps (such as WhatsApp) for case discussions. Such apps must only be used for making or confirming arrangements for appointments where a child or family has indicated this is their preferred contact method. The voice calling abilities of apps can be used for making voice calls if this is the preferred contact method. Outbound video calling must only be carried out using Microsoft Teams and consideration given to information assurance when invited to use other platforms (where there is no control over the location of Cafcass and personal data).

d) Must not use applications linked to their personal Microsoft or Google account, or those of any other provider, to transact with or store Cafcass data, to prevent data being stored in an insecure location.

e) Should note that the iPhone password must be used for hotspot use.

f) Must turn off the hotspot when not in use.

4.12 Staff using voice-only mobiles: these will be provided and set up with a PIN. This should not be removed.

4.13 Staff should exercise care and take precautions against loss or theft, whilst not endangering their own safety if challenged. Staff must also follow any other security guidance which is given. Please refer to section 2.7.p above regarding theft or loss of equipment.

4.14 Obscene or threatening calls, whether from people you know or from complete strangers, are a criminal offence. They must be reported immediately to your line manager. If a number change is required, then there is a charge if not reported to the Police. Ofcom advises: “If the caller is making direct threats to you or your family and you believe those threats to be real and immediate, then you must call 999 immediately. However, if you believe that the threats made are not immediate, then you should call your local police station (101 from any landline or mobile phone)”. See the Management of Unacceptable Behaviour Policy for further information.

5.0 Expected practice in the use of IT

5.1 All Cafcass equipment and systems support service delivery. This policy and associated procedures should be read in conjunction with the Recording and Retention Policy and Information Assurance Policy and current guidance for the effective use of tools, such as, the Cafcass case management system, laptops, tablets and smartphones for all professional tasks. Taken as a whole, Cafcass systems support fully digital working practices, including operating in a paperless manner, working remotely and flexibly and in using technology in direct work with children and families.

5.2 Staff should make full use of all the functionality available to them through Cafcass IT equipment and systems to ensure that all tasks are carried out as efficiently and effectively as possible.

5.3 Cafcass expects all staff to identify their own information technology training needs, and to discuss these as part of the PLR process, to ensure that all necessary training is undertaken.

6.0 Bring Your Own Device (BYOD)

6.1 Bring your own device (BYOD) is a service offered by Cafcass only to those identified in the table in section 3.2 to enable them to use their own devices for their work with Cafcass (e.g., mobile phones, laptops and tablets).

6.2 Those eligible for BYOD must comply with this policy and procedures in full, with the exception of clause 2.6.h which does not apply.

6.3 Access to Cafcass systems will only be provided on satisfactory completion of a cyber security and information protection questionnaire. The questionnaire will be revalidated annually and Cafcass will monitor compliance.

6.4 Those eligible for BYOD must maintain the security of their hardware by applying security and update patches within 14 days of them being made available.

6.5 Access to Cafcass systems must use multi-factor authentication (MFA).

6.6 All Cafcass activity conducted by those eligible for BYOD will be monitored by the Cafcass Security Operations Centre (SOC).

7.0 Artificial Intelligence (AI)

7.1 Artificial Intelligence (AI) tools are transforming the way we work. They have the potential to automate or enhance tasks, improve decision-making and provide valuable insights into our operations.

7.2 However, the use of AI tools also presents new challenges in terms of information security and data protection. We need to be safe and secure when using AI tools, especially when it involves the use of sensitive information.

7.3 We need to ensure that AI is used in a secure, responsible and confidential manner.

7.4 Cafcass recognises that the use of AI tools can pose risks to our operations and the children and families with whom we work. Therefore, we are committed to protecting the confidentiality, integrity and availability of all child and family and Cafcass corporate data.

7.5 When using AI we will:

a. Evaluate AI tools before use. The security of any AI tool must be evaluated before using it. This includes reviewing the tool's security features, terms of service and privacy policy.

b. Protect sensitive data. We will not upload or share any data that is sensitive, proprietary or protected by regulation, without prior approval. This includes data related to children and families, those named in proceedings, employees, finance and partners.

c. Control access. We will not give access to AI tools outside Cafcass. This includes sharing login credentials or other sensitive information with third parties.

d. Use reputable AI tools. We will only use only reputable AI tools and be cautious when using any AI tool.

e. Ensure compliance with the IT Policy. We will apply the same security practices we use for all Cafcass and child and family data. This includes using strong passwords, keeping software up-to-date and following our data retention and disposal policies.

f. Data privacy. We will exercise discretion when sharing information and only do so in line with the Information Assurance Policy.

g. Ensure that staff are aware that they remain individually responsible for any material produced, whether created wholly by or with the assistance of, an AI tool.

7.6 AI tools must not be used at Cafcass without permission being provided. This is to prevent data leakage and data breaches.