IT Policy and Procedures

Overview

This policy and associated procedures apply to Cafcass staff and all other parties who are given access to Cafcass electronic information and premises, including but not limited to technology providers, Cafcass Associates, researchers, other contractors and agents.

When individuals log on to the Cafcass IT network or a Cafcass-provided device, they automatically accept the terms outlined in this document.

IT plays a crucial role in service delivery in Cafcass. For that reason, Cafcass staff must meet and maintain a standard of use in accessing all relevant systems and data from Cafcass devices, including the Electronic Case Management System (ECMS) and its replacement the Children and Families Information System (Cafis) and all other systems in line with the case recording policy and finance and HR policies, as well as any other relevant external regulations and laws.

Owned by	Robert Langley, Head of IT and CIO
Approved by	CMT
Approved on	
Implemented	
Version	3.0
Amended	27/02/2020
Next review	March 2021 (or by projects)

Contents

1.0 Policy statement 3

2.0 Security procedures 4
Requirements 4
Working overseas 6
Passwords 7
Removable Media 7

3.0 IT Allocation Procedures 9
Allocation rules for standard IT equipment 9
Other IT equipment 10
Mobile phones (voice only) and smartphones 10
Particular needs hardware and software 10
Equipment returns 10
Equipment not to be returned 11

4.0 Mobile Phone Procedures 12
Usage 12
Mobile phones and driving 12
Security 13

5.0 Expected practice in the use of IT 14

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 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 ICT systems. The RMF will:

a) Make assessments of the potential threats, vulnerabilities and associated controls to reduce risks to people, information and infrastructure to an acceptable level. In doing so, it will ensure compliance with relevant statutory obligations and protections and will be guided by the Government Security Policy Framework and associated publications. Assessments will be made at organisational, business process and system level and will take into account the probability and impact of a risk materialising. Cafcass will use a formal risk assessment approach as recommended by Government.

b) Only permit the deployment of systems that are engineered to meet the requirements for acceptable residual risks defined at each of the assessment levels (organisational, business process and system). Compliance will be monitored continuously. Cafcass will therefore:
- Protect ICT resources from known exploits using electronic and procedural controls;
- Monitor the use of its resources so that it is aware of any failure, attack or imminent threat;
- Respond to failures, attacks or imminent threats at sufficient speed to minimise damage, gather evidence for prosecution and alert authorities; and
- Have in place recovery procedures to reinstate services that have failed.

c) Maintain 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. From time to time certain training may be a mandatory requirement.

1.3 Cafcass will normally use ICT 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 Cafcass staff and others including supplier staff. 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 Cafcass' 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 ICT 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 staff taking receipt of any equipment that allows access to Cafcass' network and other facilities.

2.0 Security procedures

This section explains how all staff members and providers must contribute to maintaining the security of Cafcass' electronic information.

2.1 All members of Cafcass staff are responsible for contributing to the security of information systems and data belonging to Cafcass. They are also responsible for reporting breaches of the policy to their managers and/or other appropriate staff members via the IT or Governance team mailboxes immediately (see 2.6 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. 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.

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 (including wireless broadband), intranet 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.

2.6.1 All those to whom this policy applies must:

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

b) Complete any mandatory or optional training as 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;

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

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

[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.

g) Not use any personal (or other non-Cafcass) IT equipment together with any Cafcass IT equipment (including Cafcass smartphones) 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 3.13 for more information on the use of removable media;

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

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

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

k) Ensure all internet use complies with Cafcass guidance, including the training module on the use of social media;

l) Immediately report all IT equipment[3] thefts and losses to:
- The Littlefish service desk (Tel. 03300 55 22 00)
- Your manager
- The Cafcass governance team

m) Immediately report all breaches of this policy to:
- The Cafcass governance team
- The Cafcass IT team
- Your manager

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

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

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

q) 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 a member of the IT team for guidance;

r) Return all IT equipment, to your line manager when leaving Cafcass' employment, and not use Cafcass IT equipment or systems after any official leaving date.

[2] Exceptions are (where they have been procured from reputable vendors): USB-connected printers, mice, screens and keyboards; VGA, DVI, DisplayPort and HDMI screens and projectors; mobile phones and other devices for charging purposes (but *only* when using a 'charge only' cable); 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 and CDs.

Exceptions may be granted by the line manager in specific cases, such as sessional workers completing casework after their employment contract end date;

s) You are responsible for ensuring that you regularly shut down (rather than sleeping) 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 2 weeks (either via the remote access service (VPN/FortiGate) or in a Cafcass office), you must ensure that when you next connect, you do so for a period of hours to enable your device to catch up with any missing updates;

t) Beware of social engineering techniques that will attempt to lure people into inadvertently infecting their system with malicious content or into compromising sensitive data. This could be done through malicious people making phone calls pretending to be from a recognised organisation (whether a person, company or government body), and requesting information or action, to steal sensitive data or infect the system. You must always be vigilant and seek advice if you suspect or are unsure whether a call is fraudulent or malicious. Another technique is 'scam' or 'phishing' emails: these are emails that look like official correspondence from a company (often a bank or phone company) but are designed to steal personal information or corrupt an organisation's IT network. You must be attentive and ensure all unsolicited emails are treated as suspicious. Any email received that has been quarantined by the email service that you are not expecting should not be released. Never click on any links contained within suspicious or unsolicited emails, and report anything suspicious to the Littlefish service desk.

2.7 Any member of staff with administrative level access to key systems (Office 365 services, Intranet or ECMS), 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.

2.8 A staff member's standard account for a system should 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 for administrative accounts.

Working overseas

2.9. All staff should obtain permission from their manager and then complete the "International Travel" service request form 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, as travel to some countries may take longer to approve than others. Make sure you list all the countries you will be visiting, even if you're 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.

2.10. 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 FCO overseas guidance published on the internet for each and every country you plan to visit[4].

Passwords

Passwords are required to ensure that Cafcass devices and systems are only used by those who should be using them.

2.11. Laptops:

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

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

c. Hello for Business secures laptops by enabling authentication in three ways:
   i. Password;
   ii. PIN; and
   iii. Fingerprint and/or facial recognition.

d. All three methods of authentication may be set up in 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.

2.12 iPhones:

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

b. iPhone encryption must be set up on receipt of a phone. Both a PIN and fingerprint recognition can be set up but only one of these is required to gain access to a Cafcass iPhone (the setting of a PIN is mandatory).

2.13 Systems:

a. There is a requirement for Cafcass and all its suppliers to have achieved Cyber Essentials as a minimum security accreditation. To gain Cyber Essentials password requirements for systems 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

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

- Memory cards (like those used in cameras);
- USB pen drives;

[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

- 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.

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

2.16 Removable media provided to Cafcass staff to use 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 devices to your laptop if it is necessary for work purposes.

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

2.18 The transfer of Cafcass information to removable media is only permitted when the removable media is correctly encrypted and there is no practical 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 who is 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.

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

2.20 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 by our disposals contractor (currently SCC) to ensure it is disposed of securely to avoid data leakage.

2.21 When the business purpose has been satisfied the contents of the removable media should be removed from the 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 Cafcass.IT@cafcass.gov.uk.

3.0 IT Allocation Procedures

This section clarifies the allocation rules for Cafcass IT equipment, user accounts and those services funded by local budgets. Each Cafcass employee is issued with a standard bundle of IT equipment (e.g. laptop, power pack, stylus pen (if applicable), iPhone and accessories).

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 local areas 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 of each end user device (i.e. laptop and phone) at any given time except in 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 budgets cover the procurement of an additional or alternative device.

Staff groups	Equipment
• Cafcass Associates	• No user account or equipment; • Required to use Egress mail service for all correspondence at Official or above
• Business Services	• Standard laptop default • Apple iPhone 6S
• Family Court Advisers • Student Social Workers • NQSWs (including those on 100-day placements)	• Touch screen laptop default • Apple iPhone 6S Plus
• All other staff including Bank Workers, CMT, OMT and corporate staff	• Standard or touch screen laptop • Apple iPhone 6S or 6S Plus • Voice only and voice with data phones Staff are offered a choice between the above. Where no preference is made a touch screen laptop and iPhone 6S Plus will be provided. The device 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 in direct proportion to the organisational need.

Note: There is a three working-day lead time service level agreement to provide equipment for new starters.

3.3 Where local teams require different equipment 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 area.

3.4 Where local 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 area.

3.5 Laptops are not provided with mobile broadband capability. They must connect to the Cafcass network by the following:

a) Fixed wired connection in a Cafcass office;

b) Cafcass office wireless broadband, where available;

c) Government department, court or agency broadband facility (e.g. GovWifi);

d) Home broadband and other public or private wireless internet connection that does not require sign in via a "landing page";

e) Any smartphone or mobile broadband device that can be used as a mobile hotspot; or

f) A Wi-Fi-specific device.

Other IT equipment

Mobile phones (voice only) and smartphones

3.6 Mobile phones and 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 and the costs covered by the local 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 HR and IT teams as reasonable adjustments. This and other specialist office equipment can be ordered via a Particular Needs Service Request and paid for out of local budgets.

Equipment returns

3.9 Any equipment including laptops, iPhones and voice only phones not actively being used by staff must be returned immediately to Littlefish by completing a service request, otherwise additional costs will be incurred. If the equipment has been swapped as part of a faulty breakfix request, Littlefish will collect this as part of the incident.

3.10 Equipment (laptops, iPhones, mobile phones and their peripherals) for those on extended periods of leave 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 3 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. Local 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

3.12 Do not return:

- Working keyboards or mice should remain on site;
- Rucksacks can be reallocated to new starters; or
- Used phone headsets (ear bud type) are to be disposed of and not reused.

4.0 Mobile Phone Procedures

This section sets out the procedures for the use of corporate mobile phones (both voice-only and iPhones) 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. The IT team will circulate monthly invoices to all managers for checking. 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 2GB 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 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. Current call charges are shown on the intranet.

4.7 Faults or damage to all phones should be reported to the Littlefish service desk.

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 and fingerprint 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) Only apps available in the Comp Portal store will be permitted on the iPhones.

c) Messaging apps (such as WhatsApp) cannot be used for case discussions. They must only be used for making or confirming arrangements for appointments where a service user has indicated this is their preferred contact method.

d) When not in use the hotspot and Bluetooth must be turned off.

4.12 Staff using voice only mobiles:

a) Mobile phones will be provided set up and with a PIN. This should not be removed.

b) If data has been included within the tariff, a password will need to be created and used for hotspot use.

c) Staff must not use applications linked to the personal Microsoft or Google account to transact with or store Cafcass data, as data can be stored in an insecure location.

d) If the mobile phone includes data, when not in use the hotspot must be turned off.

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 2.6 above regarding theft or less 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)”.

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 Case Recording and Retention Policy and Information Assurance Policy and current guidance for the effective use of tools such as ECMS, laptops, tablets and smartphones for all professional tasks. Taken as a whole, Cafcass systems support fully digital working practice, 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 training needs, and to discuss these through the PLR process, and to ensure that all necessary training is undertaken.