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 an individual logs on to the Cafcass IT network or a Cafcass-provided device, they automatically accept the terms outlined in this document and acknowledge this through the acceptance of the security notice on screen.

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 all other relevant systems in line with the case recording policy and finance and HR policies.

Owned by	Robert Langley, Head of IT and CIO
Approved by	CMT
Approved on	27/02/2018
Implemented	06/03/2018
Version	2.1
Amended	n/a
Next review	August 2018

Contents

1.0 Policy statement

1.1 Cafcass depends on secure and reliable technology, support and training to deliver its services. Maintaining IT systems in good working order is crucial as services to children depend upon accurate, immediate 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 deploy 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.
- Have in place recovery procedures to reinstate services that have failed.

c) Maintain staff awareness of the potential vulnerabilities of systems and therefore the importance of implementing procedures and of regular training.

1.3 Cafcass will normally use ICT services provided by external suppliers. It will engage with suppliers throughout the system life-cycle 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 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 (see 2.6k 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 will 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 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 tagged, 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 All those to whom this policy applies must:

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

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

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

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

e) Not use Cafcass' time, facilities, equipment or supplies for 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.

f) Not use any personal 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 or transfer Cafcass data;

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

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

i) Logout of or lock your computer or smartphone when not in use or left unattended, even for short periods;

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

k) Report, as soon as practicable, all IT equipment thefts and losses, and all breaches of this policy to:[3]

   a. The Fujitsu service desk (Tel. 0344 875 0410)

   b. The Cafcass governance team

   c. The Cafcass IT team

l) Keep all doors to comms rooms and cabinets locked and secured;

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

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

o) Follow the relevant process on the intranet in order to gain access to systems;

p) Return all IT equipment to the line manager when leaving Cafcass' employment, and not use Cafcass IT equipment after any official leaving date. Get permission from line managers before taking any equipment abroad to use

q) You are responsible for ensuring that you regularly shutdown (rather than hibernating or 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 [RAS] 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.

r) Beware also of '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 elicit personal information or corrupt an organisation's IT network. You must be vigilant 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

[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.

be released. Never click on any links contained within suspicious or unsolicited emails, and delete the email immediately. If in doubt, you should seek advice.

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 other users access rights, will be required to go through additional security vetting to obtain SC clearance 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.

3.0 IT allocation procedures

This section clarifies the allocation rules for Cafcass IT equipment, user accounts and those services funded by local budgets.

Allocation rules for standard IT equipment

3.1 The table below outlines the allocation of standard IT equipment in relation to 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 end user device (i.e. laptop) 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 device.

Staff groups	Equipment
Non-Cafcass staff Associate Family Court Advisers	No user account or equipment; required to use Egress mail service for all Official correspondence
Business Services	Standard laptop default
Family Court Advisers Student social workers, NQSWs (including those on 100-day placements)	Touch screen laptop default unless use of the standard laptop is support by an Access to Work/Occupational Health Assessment
All other staff including bank workers, CMT, OMT and non-practice staff	Standard or touch screen laptop Staff offered a choice between the above, where no preference is made a touch screen laptop will be provided. The device provided will be subject to availability depending on stock levels at the time

Note: There is a five-day lead time 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 with the cost of the equipment funded by that local area, unless it is for reasons outlined and supported by an Access to Work or occupational health report, in which case certain technical equipment and software may be available free of charge depending on suppliers and associated contractual terms.

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 via either:

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. Gov WiFi

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

f) A WiFi-specific device.

Other non-standard IT equipment

Mobile phones (voice only) and smartphones[4]

3.6 Mobile phones and smartphones are available by manager request, the provision of which is managed by the IT team. The allocation of a mobile phone is dependent upon an employee's job role, not the individual. Newly-issued smartphones are supplied with a headset and charging cable.

3.7 Mobile phone accessories such as protective cases, screen protectors and additional/replacement headsets can be ordered with the costs covered by the local area.

Particular needs hardware and software

3.8 Particular needs hardware and software (e.g. specialist Keyboards, Dragon software) are available to individuals with particular needs identified by recommendations within formal Access to Work or Occupational Health assessments and subsequently agreed by HR and IT teams as reasonable adjustments. No additional funding is required for all formally documented reasonable IT adjustments as they are covered as standard by the existing Fujitsu contract. Note: other specialist office equipment is procured and paid for by the local office.

Equipment returns

3.9 Any equipment that is not being actively used by staff must be returned immediately to Fujitsu by completing a ServiceNow request form, otherwise additional costs will be

[4] Smartphone Frequently Asked Questions and Smartphone data usage FAQs can be found on the Cafcass intranet.

incurred. Note: smart phones and mobile phones should be returned to the IT team in the Leeds office, as in section 4.16.

3.10 Equipment (laptops/tablets/smartphones/mobile phones) for users on extended periods of leave must be returned unless specific local agreement is made with individuals to support 'keeping in touch' arrangements. Equipment will be reallocated to such users upon their return to work, noting there is a 5 day lead time for fulfilment of the service request.

3.11 Each Cafcass user is issued with a standard bundle of IT equipment e.g. laptop, power pack, stylus pen, etc. Local budget centres will be charged if the issued equipment is not returned at the point of staff leaving or where damaged equipment is not returned. Local budgets will also be charged for replacements due to loss or damage (including laptops and smartphones) Line managers will be informed of loss of or damage to IT equipment. All current costs are maintained on the intranet.

Equipment not to be returned

3.12 Do not return working universal docking stations (PR07s), keyboard, mice or rucksacks to Fujitsu, as they are owned by Cafcass**.** Used phone headsets (ear bud type) to be disposed of and not reused.

Return surplus PR07s and their associated cables and power packs to the NBC from where they will be reallocated on approval by the IT team.

4.0 Mobile phone procedures

This section sets out the procedures pertaining to the use and acquisition of corporate mobile phones (both voice only and smartphones) in Cafcass and is deemed to have been accepted on receipt of a phone, allocated as in section 3.

Usage

4.1 Line managers are accountable for monitoring the responsible use of smartphones and mobile phones (both voice and data usage) and for taking appropriate action in the event of misuse. The IT team will circulate on a monthly basis invoices for checking and 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 The user is responsible for all calls and data usage on the smartphone or mobile phone provided, and therefore should not loan or transfer to another user or allow unauthorised wireless connections that allow non-Cafcass staff or devices to use 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. The office directory on the Cafcass intranet contains the current mobile numbers. Users should also include their mobile number in email signatures.

4.4 Users exceeding the 2GB monthly mobile data limit will be audited and where appropriate may be moved to an alternative tariff to accommodate higher levels of legitimate business use. Text alerts are sent out to those mobile users whose data limit is close (80% used) to being exceeded. Colleagues should email cafcass.it@cafcass.gov.uk when this text is received if this is a cause for concern.

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 intranet.

4.7 Faults with smartphones should be reported initially to the service desk. Faults with voice-only mobile phones should be referred to the Cafcass IT team to resolve.

Mobile phones and driving

4.8 It is illegal to use a hand held mobile device when driving. Cafcass does not permit staff to use hand held mobile phones or smartphones when driving.

4.9 It is not illegal to use a hands-free mobile phone or smartphone whilst driving a vehicle. However, the user must ensure that they remain able to drive safely with due care and attention and remain in control of their 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 Android smartphones:

a) Must install anti-virus software. Staff must not change settings within the anti-virus application to prevent it from carrying out scans of the device;
b) Only Citrix Secure apps should be used to transact or store Cafcass data. Apps should only be installed from the Worx store (with the exception of Citrix Securehub);
c) The use of voice dictation is permitted but can only be used if the setting to store voice data against the Google account is disabled, by following published guidance.

4.12 Staff using Windows smartphones:

a) Must not use applications linked to the personal Microsoft account to transact with or store Cafcass data, as data can be stored in insecure locations. This includes the use of Cortana if voice dictation is used.

4.13 Staff using Android or Windows smartphones

a) 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.
b) When not in use Bluetooth must be turned off.

4.14 Staff should exercise care and take precautions against theft, whilst not endangering their own safety if challenged. Staff with voice only mobile phones should set up a PIN on their mobile to prevent unauthorised use. Staff with smartphones must use the stipulated password regime and follow any other security guidance which is given. Refer to section 2.6k above regarding theft or loss of equipment

4.15 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 and the mobile phone company. 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)”.

Working overseas

4.16 Staff should obtain permission from their manager before taking a mobile outside the UK and should read the FCO overseas guidance published on the internet. Note that data tariffs for international roaming, especially outside the EU, can be very high (and

may be uncapped) check our current network provider guidance and additional permission should be sought for such use. Where possible, Wi-Fi should be used. Switch off data roaming before you leave the UK, otherwise your smartphone will automatically seek out an internet connection when you reach your destination and you may start using data without realising it.

Return of equipment

4.17 Mobile phones and smartphones must be returned to the IT team based in the Leeds office if the user goes on extended leave or ceases employment with Cafcass. Bank Worker mobile phones similarly need returning when ceasing the current period of work.

5. 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 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 Cafcass expects all staff to identify their own training needs and to ensure that all necessary training is undertaken.

5.3 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.