

UNCLASSIFIED



IT SECURITY POLICY

What is in this policy?

This Information Technology (IT) Security Policy applies to Cafcass, and all other parties who are given access to Cafcass electronic information and premises, including Cafcass staff, business users, Cafcass technology providers, self-employed contractors, other contractors and agents. The policy explains how all staff members and providers must contribute to maintaining the security of Cafcass' electronic information.

UNCLASSIFIED

Owner: IT Department

Issued:

Approved by: Cafcass CMT

Version no: 1.1

Next review: November 2009

Ref:

CONTENTS

WHAT IS IN THIS POLICY?	1
CONTENTS.....	2
INTRODUCTION.....	3
<i>Confidentiality.....</i>	<i>3</i>
<i>Integrity.....</i>	<i>3</i>
<i>Availability.....</i>	<i>3</i>
SECURITY POLICY	4
POLICY REQUIREMENTS FOR ALL STAFF	4
ACCEPTABLE USE.....	4
POLICY REQUIREMENTS FOR OFFICE MANAGERS.....	6
IT EQUIPMENT SECURITY	6
IT COMMS ROOM (“ELECTRICAL CLOSETS”) SECURITY.....	6
POLICY REQUIREMENTS FOR HUMAN RESOURCES.....	6
GUIDANCE FOR ALL STAFF IN UNDERSTANDING AND ENSURING NETWORK SECURITY	7
ACCESS	7
LOCAL AREA NETWORK SECURITY	7
WIDE AREA NETWORK SECURITY	8
PASSWORD SECURITY	8
MOBILE DEVICE SECURITY	8
LAPTOPS	8
BLACKBERRIES	8
INTERNET SECURITY.....	9
GLOSSARY	9
APPENDIX A – DOCUMENT HISTORY.....	10

Introduction

Cafcass relies on the integrity and accuracy of its information in order to deliver our services. Therefore it is important that all our staff members¹ and technology providers understand the importance of ensuring the accuracy and security of corporate, case related and other sensitive information. This policy explains how all staff and providers must contribute to the maintenance of the security of Cafcass' electronic information.

When a user logs on to the Cafcass IT network or a Cafcass provided machine or device they are automatically accepting the terms and conditions outlined in this document.

The majority of Cafcass' information is stored on IT systems as files, and as such must be protected not only from unauthorised access, but also from inappropriate or untimely destruction or unauthorised change. Tackling the threat to IT and systems security is a complex and often difficult task which includes staff awareness, control of access, detection of unauthorised activities, recording and investigation of breaches, and where necessary, disciplinary procedures.

As well as protecting the data within computer systems, it is also necessary to protect the systems themselves from misuse and abuse. The objective of IT and systems security is to preserve:

- **Confidentiality**

It is necessary to restrict access to information to those with specified authority to view it, and where appropriate, to change it.

- **Integrity**

It is essential to ensure that systems are operating as specified, that authorised users are properly interpreting information and that the data held are accurate and have not been altered except through authorised processes.

- **Availability**

It is essential that information is delivered to the user where and when it is required.

¹ The term 'staff member' is used throughout this policy to refer to all employed, bank staff, agency, and self-employed contractors and those persons listed on the front cover to whom this policy applies.

Security policy

Cafcass' IT Department will provide adequate technical protection and confidentiality measures for all Cafcass electronic data and proprietary software systems, whether they are held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration controls.

All Cafcass staff members 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 or other appropriate staff members.

Cafcass will ensure Internet usage is monitored, including the length of use and sites visited. Cafcass will only monitor email content where necessary to comply with this policy and to prevent the use of the system for discriminatory purposes and/or harassment and/or the commission of a criminal offence.

Cafcass will treat violations, repetitive breaches, or behaviour which is clearly illegal or offensive or in breach of policy, as a disciplinary matter.

Policy requirements for all staff

Acceptable use

Electronic equipment (mainly laptops, thin client and desktop computers and Blackberry handhelds), internet, intranet and email access provided by Cafcass are intended for Cafcass business use, but limited access for personal use is allowed. Use of Cafcass' time, facilities, equipment or supplies for an employee's or contractors' private business is prohibited.

Cafcass encourages staff to use the internet, intranet and email, because they make communication and research more efficient and effective. IT equipment and the data it contains is a valuable asset of Cafcass. Every staff member is responsible for reducing the possibility of theft, damage or unauthorised access.

Cafcass IT, data and telecommunication systems must only be used for business related and sanctioned purposes.

Personal IT equipment and unauthorised electronic devices not belonging to Cafcass should not be used together with any Cafcass IT equipment. This includes USB flash drives and PDA devices.

Personal IT equipment must not be used to work on any Cafcass document which is or would be marked as Protect or higher (including all case related information).

These must be contained within the secure environment provided by the Cafcass network. Where it is available the protective marking of documents must be managed in line with the Case Recording Policy.

To protect network security:

- Usernames and passwords must not be shared by users;
- Usernames and passwords should not be written down;
- Usernames will consist of initials and surname;
- Users must logout or lock their computers when they are not in front of their computer;
- Remote connection to any Cafcass machine through another third party product such as GoToMyPc is prohibited;
- Users must not remotely connect to any Cafcass machine from a non-Cafcass machine; and
- No software whatsoever (including freeware and shareware) is to be downloaded or installed on any Cafcass machine without the authorisation of the IT department. Failure to comply may lead to disciplinary proceedings.

To protect security of hardware, laptops:

- Must not be left in view in cars when parked;
- Must not be left in a vehicle overnight;
- Must be locked away out of view when left in the office;
- Must have up to date anti virus and firewall protection by regularly connecting to the network;
- Smart cards/ security dongles and laptop must be stored separately; and
- Must only be used for business purposes.

The internet can be used to communicate and exchange information as long as usage complies with all applicable [legislation and guidance](#) including those:

- Governing the management of protectively marked data;
 - Governing the import and export of technology, software and data;
 - Restricting the use of telecommunications technology and encryption;
 - Governing the transmission of data across national borders; and
 - Copyright, licensing, trademark, and advertising laws.
-

Policy requirements for Office Managers

IT equipment security

Office management are responsible for assessing the vulnerability of their equipment to theft or unauthorised access. If they deem the equipment to be vulnerable to either, they are required to take appropriate protective actions.

All IT equipment thefts, losses and breaches of this policy must be reported to the IT department at the National Office.

Physical security of computer equipment will comply with the requirements as detailed below.

IT comms room (“electrical closets”) security

All sites and offices have "electrical closets" containing data, voice and LAN communications connections. Although access in some offices is normally controlled by the IT Department, these areas should be reviewed to ensure that adequate access controls are in place. Unauthorised entry to these areas and tampering with the equipment could affect the operation of your computer systems and could allow serious security breaches.

Doors to the room and cabinets will be kept locked and secured with a key lock, combination lock, card access system, or some other type of lock. Access to the room should be restricted to only those people that need to have access to the equipments to perform their normal job functions. A list of all people with access to the room must be maintained, including those people requiring access but not directly affiliated with the area.

Access to the comms room must be treated as restricted and controlled.

All contractors working within the comms room are to be supervised at all times and the IT Department is to be notified of their presence and provided with details of all work to be carried out, at least 48 hours in advance of its commencement.

Policy requirements for Human Resources

The IT Helpdesk must be notified of all employees leaving the organisation's employment by the HR department. The IT Helpdesk will then ensure the removal of the employee's rights to all systems.

Guidance for all staff in understanding and ensuring network security

Access

- Access to all computers connecting to the Cafcass network is controlled with the use of user login IDs and passwords.
- Only Cafcass employees or their contracted agents will be permitted access to Cafcass IT systems. Agents contracted to Cafcass will be required to accept the Cafcass IT Security Policy as part of their terms of engagement.
- Users will only be given sufficient rights to systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
- Users requiring access to systems need to make a written application on the [forms](#) provided by the IT Department or through the catalogue provided by Cafcass' IT supplier.
- It is unlikely that any one person will have full rights to any system. The IT managed service supplier will control network and server passwords and the system administrator will assign system passwords.
- Access to the network and to laptops and systems will be by individual username and password:
 - All users will have an alphanumeric password of at least 12 characters, with a mix of upper and lower case and letters, numbers and symbols; and
 - Passwords will expire every 90 days and must be unique.
- Auditing will be implemented on all systems to record login attempts and failures, successful logins and changes made to all systems.
- Regular use of the generic administrative username on IT systems is prohibited.
- Default passwords on systems will be changed after installation.

Local Area Network security

Hubs and switches

LAN equipment, hubs, bridges, repeaters, routers, switches will be kept in secure comms rooms. Comms rooms will be kept secured according to the policy statement above ("IT comms rooms security").

Computers

Users must logout or lock their computers when they are not in front of their computer.

Monitoring software

The use of LAN analyser and packet sniffing software is prohibited unless authorised by the IT Department.

Wide Area Network security

Direct wireless access to the LAN (Local Area Network) is prohibited.

Remote access to the Cafcass network is through the VPN only and should pass through the IT network's router and firewall.

All bridges, routers and gateways will be kept locked up in secure areas.

All connections made to the organisation's network by outside organisations (third party suppliers) will be logged.

Password security

- All passwords will lock after 5 invalid attempts to use them.
- The password lock shall remain in-place for 24 hours. (This means the lock placed after 5 invalid attempts will be removed after 24 hours; resetting a password will automatically remove this lock before the 24 hour time limit)
- All user-level passwords (e.g. email, web portal, desktop computer, laptop, etc.) will be changed at least every 90 days.
- All user level passwords need to be a minimum length of 12 characters and contain a mixture of upper and lower case letters and numbers.
- User passwords should not be disclosed via electronic means (e.g. inserted into email messages, unless encrypted channels are used).
- Password sharing is prohibited.
- A password must be changed as soon as it is or suspected to be known to another individual.
- If password must be written down, it must be written down and stored away from any Cafcass IT equipment.

Mobile device security

Laptops

Cafcass has a large number of network able and encrypted laptops. It is important that these machines are tracked at all times and if lost or stolen reported to the IT department immediately. The laptops are configured with firewalls and anti-virus software. The anti-virus software is updated automatically and periodically.

Blackberries

- The pin-2-pin option is not permitted from or to Cafcass owned or operated devices.
-

- The Blackberry web client is configured to use the Cafcass internet provision, so is permitted.
- The Blackberry Desktop re-director software is not permitted, the only route for mail to reach the Blackberry is to use the Cafcass provided BES service (this ensures appropriate security settings are correctly applied).
- Cafcass Blackberry devices should not be attached to non-Cafcass owned laptops or desktop PCs.
- Lost or stolen Blackberries must be reported to the IT helpdesk and the IT department immediately.
- Blackberries must be configured with a user password, which should be managed according to the statement above (“password security”).

Internet security

- Permanent connections to the internet will be via the means of a firewall to regulate network traffic.
- Permanent connections to other external networks, for offsite processing and other activity, will be via the means of a firewall to regulate network traffic.
- Network equipment will be configured to close inactive sessions.
- Workstation access to the Internet will be via the organisation’s proxy server and website content scanner.
- Cafcass’ email content scanner will scan all incoming email.

Cafcass has the right if it wishes to have access to read any matter sent or received by employees using the Cafcass network.

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 computer system, email or other technical resource, whether or not they have been marked confidential, at any time, without the permission of the employee, and without notice.

Glossary

IT is short for Information technology

NO is short for National Office

In the context of this policy, **Management** is defined as Cafcass Directors, Operational Directors, Area Business Managers and Heads of Service Managers or their deputies as nominated from time to time

The **internet** is the world wide interconnected network of computers that allows the exchange of information and electronic mail.

An **internet user** is defined as anyone (employees, contractors, customers, etc.) using the Organisation's resources to access the Internet.

PDA Personal Digital Assistant, electronic diaries and other such devices.

Email is a method of exchanging messages with other parties over an electronic network.

Spamming is the intentional distribution of multiple messages to a large number of recipients. This is in direct contravention to 'netiquette' protocol and monitored by ISPs, which have the power to disable the sender's registered account.

Blackberry is a wireless handheld e-mail/phone device.

ISP stands for Internet Service Provider

Appendix A – Document history

Date	Version	Changes / Comments	Author
12/11/08	0.1	IT Security Policy	Herbert Macaulay
13/11/08	0.2	Amended for final review and publication	Rob Langlely
19/11/08	0.3	Reviewed and amended	Chelsey Bonehill
21/11/08	0.4	Final version for approval	Rob Langlely
15/12/08	0.5	JS/JB changes approved	Rob Langlely
19/12/09	1.0	Final Version for Implementation (consistent with Information Assurance Policy)	Colette Beech (QA)
27/04/09	1.1	Further amendment and clarification	Rob Langlely