

INFORMATION ASSURANCE POLICY

Cafcass is required by law to manage our information assets effectively. This document provides the policy framework through which effective management of records can be achieved and reflects the principles set out in the Case Recording Policy. This policy describes what Cafcass does and intends to do with respect to its information and records.

Owner:	Corporate Governance Jasvinder Jassal	Issued	April 2010
Approved by:	Anthony Douglas	Version no:	2.2
Next review date:	December 2010	Ref:	

CONTENTS

NO	ITEM	PAGE NO
1.0	Introduction	4
	Scope	5
	Why do we need to Manage our Records?	5
	Regulatory Requirements	6
2.0	Roles and Responsibilities	6
	Relationship with Existing Policies	8
3.0	Record Keeping Standards	8
	What is a Record?	9
	Record Keeping Standards and Requirements	9
	Emails	10
	Version Controls	10
	How Long do we need to keep a Record?	10
	Security and Access of Records	11
	Keeping Track of Records	12
	Archive	13
	When and How to Dispose of Records	13

APPENDIX

NO	ITEM	PAGE NO
1.0	Recommended Retention & Disposal Practice	15
2.0	Protective Marking Schedule	26
3.0	Desks Clear of Confidential Material Policy	30
4.0	Cafcass Premises Security Procedures	33
5.0	Managing Emails Guidance	37
6.0	Reporting Data Breaches	43

1 Introduction

Reliable and accurate information is critical to proper decision making in Cafcass. This makes information a critical business asset that we need to protect. Information Assurance (IA) provides this protection by managing risks to the availability, integrity and confidentiality of information so that our business always functions effectively. Records management is the practice of ensuring that a record is managed through its full life cycle - creation, maintenance, managing its use, storage, retrieval and final disposal of the record. Essential elements include the approved Records Control Schedule, robust training of those responsible for implementation, and careful execution of the disposal of Cafcass records.

Cafcass is required by law to manage our information assets effectively. This document provides the policy framework through which effective management of records can be achieved and reflects the principles set out in the Case Recording Policy. This policy describes what Cafcass does and intends to do with respect to its information and records.

In addition specific requirements on the creation and management of records are set out in the:

- Data Protection Act 1998 (DPA)
- Freedom of Information Act 2000 (FOIA).
- National Information Assurance Strategy 2007 (NIAS) 2007: the Central Sponsor for Information Assurance (CSIA), part of the Cabinet Office¹
- The Manual of Protective Security (MPS)²:

¹ This was published by the Central Sponsor for Information Assurance (CSIA) in 2007 and sets out how the Government UK should approach information risk management. It aims to make Government better able to deliver public services through appropriate use of ICT; strengthen the UK's national security by protecting information and ICT at risk of compromise; and enhance the UK's economic and social well-being as government, businesses and citizens realize the full benefits of ICT. Available at www.cabinetoffice.gov.uk/csia/nationaliastrategy.aspx.

² The Cabinet Office Security Policy Division issues this document on the authority of the Official Committee on Security (SO). The document provides guidance that helps Government departments and agencies and other organisations discharge their security responsibilities by protecting the confidentiality, integrity and availability of assets used during the conduct of Government business.

- Code of Connection for the Government Secure Intranet (GSI CoCo)³:

1.1 Scope

This policy applies to the management of all operational case and non-case information and records, created, received or maintained by staff at Cafcass in the course of carrying out their corporate functions.

What is a record?

For the purposes of this policy records are defined as:

*'Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.'*⁴

Examples of items that can be records include the following:

- Administrative records (including HR, estates, financial and accounting records, contract records, litigation and records associated with complaint handling);
- Photographs, slides and other images;
- Computer files (including word processed documents, databases, spreadsheets and presentations);
- Electronic data and mail messages;
- Diaries;
- Brochures and reports;
- Minutes from meetings;
- Maps and plans;
- Audio, videocassettes and DVDs.

The Management of service user records is covered in the Case Recording Policy and there is some necessary overlap. The principles of this Information Assurance policy apply to all records.

³ The document aims to develop the trust required both within and between Government Secure Intranet (GSI) communities by setting down a minimum set of security standards that organisations must adhere to when joining the GSI. It is available at: www.cesg.gsi.gov.uk/bookstore/title.html.

⁴ Definition taken from the *international standard* Information and documentation-Records management ISO 15489-1:2001

1.2 Why do we need to manage our records?

Efficiently maintaining our records supports Cafcasses core functions, to comply with its legal and regulatory obligations and to contribute to the overall management of the organisation. Records are a valuable corporate asset that, by their retention and re-use as evidence of decision-making and business activity, can improve both the efficiency and effectiveness of an organisation.

By making and managing records Cafcass can ensure that it has available to relevant staff all the information they need to carry out their roles. This can improve

- the quality of decision-making ;
- the quality of business activity;
- long term planning;
- Compliance and meeting audit requirements;
- quality reporting; and
- fast and accurate customer service.

1.3 Regulatory requirements

Cafcass works in a regulatory environment influenced by many factors, these include but are not limited to:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Criminal Justice and Court Services Act (2000).
- Environmental Information Regulations 1992 & Environmental Information Regulations 1998
- The Human Rights Act 1998
- The Lord Chancellors Code of Practice on the Management of Records
- BS ISO 15489 The International Records Management Standard
- ISO 27001. Specification for information assurance Systems
- HMG Manual of Protective Security

2 Roles & Responsibilities

2.1 Responsibilities

Cafcass has a corporate responsibility to maintain its records and its record keeping system in accordance with the regulatory environment. Responsibility for records lies with all Cafcass staff who create, hold and manage records.

Line Managers at all levels have responsibility for ensuring that:

- national policies are adhered to and local procedures are in place to enable compliance; and

- that records management including reviewing, tracking of files and destruction is carried out in accordance with records management policy and standards.

Overall responsibility for the corporate records management programme is with the members of the Corporate Management team. The Accounting Officer (the Chief Executive for Cafcass) - has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. A Senior Information Risk Owner (SIRO) supports this responsibility. The day-to-day duties are delegated to the Information Asset Owners (listed below), Information Assurance & Data Handling Officer, and the IT Security Officer.

Cafcass has in place a SIRO, the Director Bruce Clark. The SIRO is the focus for the management of information risk at a senior level. The role of the SIRO is to lead and foster a culture that values, protects and uses information for the public good, advise the Cafcass Accounting Officer on the information risks via annual risk assessments of performance.

Cafcass has now assigned Information Assets, defined as information of value which is owned and/or used by the various business areas (data sets, databases and or ICT systems) to the following Information Asset Owners (IAO):

Christine Banim, Operational Director	Case & Complaints Records
Jabbar Sardar, Head of Human Resources	HR & Health & Safety Records
Naomi Lawson, Head Of Communications	Public Relations Records
Julie Brown Head of Finance	Finance Records
Darren Scates, Head of IT	IT enabled Information Assets (ITSystems)

The role of IAOs is to

- Lead and foster a culture that values, protects and uses information for the public good by taking visible steps to support and participate in Cafcass' plan to achieve and monitor the right culture, across Cafcass and its partners.
- Know what information Cafcass holds and how it is used up to date, by approving and minimising transfer while achieving the business purpose, approving arrangements so that information put on removable media like discs or laptops is minimised and protected and approving the disposal mechanism for paper or electronic records from their asset area.
- Know who has access to the asset information and ensures their use is monitored
- Understand and address risks to their asset and provides assurance to the SIRO.

- Ensure the asset is fully used for the public good including responding to requests for access.

Each IAO has categorised and classified all assets according to the DCSF Impact Level tables. This can be found in Appendix 1 of this policy, and Appendix 5 of the Case Recording policy. Appendix 2 provides further guidance on the control, transportation and disposal relating to the conditions set out by the protective markings. All documents should be assigned a marking of either 'Unclassified; Protected; Restricted; Confidential'. Protective markings must be placed in the header of each page of each document (note that this will be prompted on the Flex system).

The IT Security Officer will provide advice on IT Security issues, based on the Cafcass IT Security Policy to the SIRO, IAOs and Information Assurance & Data Handling Officer.

The role of the Information Assurance & Data Handling Officer is to work with the SIRO to co-ordinate Cafcass' overall information risk approach, ensuring that professional support and advice is offered to the organisation. The officer will provide expertise in the relevant legislation, ensuring that staff understand their legal obligations and realise potential opportunities. All staff are required to undertake training to enable a greater understanding of information assurance and their responsibilities; further detail will be distributed by the Information Assurance & Data Handling Officer.

Staff are required to read and comply with the guidance contained in this policy. Staff are to comply with instructions contained in this policy or subsequently issued by SIROs, IAOs and the Information Assurance & Data Handling Officer at all times – failure to do so may amount to gross misconduct resulting in disciplinary action.

IAOs, the Information Assurance & Data Handling Officer and IT Security Officer are available for guidance and advice on specific Information assurance issues.

2.2 Relationship with existing policies

This policy has been developed alongside and within the context of the following Cafcass documents:

- Data Protection Policy Data Protection Act 1998: Section 7 Subject Access Requests
- Freedom of Information Policy
- Case Recording Policy

- IT Security Policy

3 Record Keeping Standards

3.1 How to meet Record Keeping Standards

A record should be reliable, it should reflect correctly what was decided or what action was taken and should be able to support the needs of the organisations business.

Record management procedures and practices should result in records, which have authenticity, reliability, integrity and usability.

Description:	Definition:	To Meet this Standard:
Authentic record	An authentic record can be proven to be credible and authoritative so that evidence can be safely derived from it.	Each office will set up and document procedures that control the creation, receipt, transmission, maintenance and disposal of records in accordance with National policies and procedures. Record creators will be identified and records protected from unauthorised addition, deletion, alteration, use and concealment.
Reliable record	A reliable record is one whose content can be trusted as a full and accurate representation of the transactions, activities or facts they concern.	Records must be created at the time of the transaction or activity or soon afterwards (timeframes may be set in relevant policies). They should be created by staff that have direct knowledge of the system used within Cafcass to complete the activity wherever possible.
Integrity of a record	The integrity of a record refers to its being complete and unaltered	Records must be protected against unauthorised alteration. Local offices must have procedures to specify what additions/alterations can be made and by whom, in line with Cafcass policy (e.g. Case Recording Policy). Any changes to a record should be clearly indicated. Records need to be kept secure and held in a robust format, which remains readable for as long as the record is required.
Useable record	A useable record is one that can be located, retrieved, presented	Records must be arranged in a record keeping system in accordance with

NOT PROTECTED	Information Assurance Policy
------------------	------------------------------

	and interpreted.	national policy. Types of file referencing systems include alphabetical, numerical, alphanumeric and keyword. Irrespective of the type of filing system chosen in the office, it is essential that it is simple and easily understood by the users of the system, as well as being consistent with national policy.
--	------------------	--

All documents should be assigned a marking of either 'Unclassified; Protected; Restricted; Confidential'. Protective markings must be placed in the header of each page of each document (note that this will be prompted on the Flex system). See Appendix 1 and 2 for further information, many of Cafcass records have been classified by the IAO already. For further information contact the Information Assurance & Data Handling Officer.

In order for Cafcass to comply with the successful management of its records a *Desk Clear of Confidential Material Policy* and *Cafcass Premises Security Procedures* is in place. Please see Appendices 3 and 4.

E-mails

E-mails should be treated in the same way as you would treat any other form of recorded communication. E-mails are subject to Data Protection and Freedom of Information legislation and can also form part of a corporate record. Cafcass staff should be aware that e-mails could be used as evidence in legal proceedings and may be released to the public in response to a FOIA request.

It is the responsibility of all members of staff to manage their emails in order to comply with Data Protection Principles and Freedom of Information legislation. The *Managing e-mails Guidance* (Appendix 5) provides further information and best practice tips on how to manage e-mails.

Version Controls

It may be necessary to keep a record of successive versions of items. An example is in policy development when successive drafts of a document must be kept to provide adequate evidence of the process, and a record of changes. See the Policy Development Framework and the Information Assurance & Data Handling Officer for further information.

--	--

3.2 How long do we need to keep a record?

The length of time a record is kept is determined by assessing:

- The statutory and regulatory guidelines;
- Business and accountability requirements; and
- The risks associated with keeping or disposing of the record at any particular point in time.

Disposal guidance and a comprehensive retention schedule for non – case records at Cafcass can be found in section 3.7 and Appendix 1. Please refer to the Case Recording Policy for the retention of case records. Cafcass has considered the rights and interests of all stakeholders when deciding on how long records need to be maintained. Statutory/regulatory guidelines may demand that the record be kept for a minimum time, and have been followed where applicable. Records that are no longer required should be eliminated as early as possible in a systematic manner.

3.3 Access to Records

The broad principles on access rights, conditions and restrictions of records are drawn from legislation covering Privacy, Data Protection, Security and Freedom of Information. Records may contain personal, commercial or operationally sensitive information. In some cases access to the records or information about them, should be restricted.

All records must be kept securely, and in accordance to their protective marking classification. Safeguards must be in place to ensure the required levels of confidentiality are met. See Appendix 1 and 2 for further detail on what classification, and therefore any restrictions on access, has been assigned to Cafcass records.

Records and documents that require a protective marking of PROTECT or RESTRICTED should be identified as such, only where specifically required by a business need or the regulatory environment. It should be noted that adding a restriction to a record does not necessarily prevent access to the record or the information contained in the record. The Freedom of information Act 2000 is intended to promote a culture of openness and accountability amongst public authorities. It promotes the disclosure of information, unless an exemption applies and even then a public interest test may be applied. See the Cafcass Freedom of Information policy for more details on the FOIA. Irrespective of any restrictions made to Cafcass records, the Data Protection Act and the Freedom of Information Act could still result in the information having to be released.

Cafcass staff should be aware of guidelines regulating who is allowed access to records and in what circumstances and also be aware of their responsibilities for compliance with security procedures for electronic records.

Cafcass staff should understand:

- Their responsibility under the Data Protection Act for handling records about named individuals;
- Their contractual duties relating to confidential information;
- The process for restricting access to records; and
- The circumstances where Cafcass records should be restricted taking into account Cafcass's obligations under the Data Protection and Freedom of Information Act.

The guidance contained in Appendix 6 *Reporting Data Breaches Cabinet Office Guidance* outlines the action Cafcass is required to take when a suspected breach of the Data Protection Act occurs.

Staff are required to inform their line manager, the appropriate IAO and the Information Assurance & Data Handling Officer **as soon as the breach is suspected**. Information Assurance & Data Handling Officer, together with the IAO, will assess the extent of the breach and take appropriate action.

3.4 Keeping track of records

The movement of records should be documented to make sure that items can always be found when required.

The tracking of the movement, location and use of records is required to:

- Enable retrieval of a record;
- Prevent loss of records;
- Maintain an auditable trail of record transactions (capture, registration, classification, indexing, storage, access, use, migration, transfer or disposal); and
- Enable to identification of individual records where systems have been combined or migrated.

Procedures must be in place in each Cafcass office for the tracking of records, and be consistent with relevant Cafcass policy (e.g. Case Recording Policy for case files). This can be done via a paper or an electronic audit trail. The system should track the transfer of records between departments/offices and authorised external organisations including external archives.

3.5 Archive

Records should be transferred to the Archive (internal or external) once their current and semi-current life has expired. Records of long-term historical or evidential value must be transferred to the Archive and not be stored in offices. It is essential to keep track of all records that have been put into archive Cafcass has a contract for archiving documents with [TNT](#). Each record put into archive should be easily

retrievable. It is the responsibility of all Cafcass staff involved in record management to locate these records and keep robust management systems.

3.6 When and how to dispose of records

The retention schedule for non-case records at Cafcass is attached in Appendix 1. The retention schedule states the retention period (timetable) of each type of record captured by the business area.

The retention schedule details the process of determining whether to keep, move or destroy a record in accordance to regulatory retention schedules. Records are disposed of when:

- The record is no longer required;
- No work is outstanding; and
- No litigation, investigation or access request is current or pending which is relying on that record.

The date the retention period starts is clearly indicated for each business area.

Destruction of records at the end of the retention period should be authorised and must be disposed of in a manner appropriate to their confidentiality or sensitivity. A record should be held of which items have been destroyed together with the appropriate authorisation signatures of senior management and evidence that the destruction has taken place, for example a certificate.

Please seek guidance from the Information Assurance & Data Handling Officer or IT Security Officer of how to dispose of records, and records on various formats eg video, DVD, Cassette.

INFORMATION ASSURANCE POLICY

Appendix 1

Appendices	
1	Retention & Disposal Practice
2	Protective Marking Schedule
3	Desk Clear of Confidential Material Policy
4	Cafcass Premises Security Procedures
5	Managing Emails Guidance
6	Reporting Data Breaches

Cafcass Retention Criteria for HR Records

Known Best practice - National Archive CIPD, Information Commissioner, ACAS& Business Link

Description	Disposal	Impact level - Protective Marking
Written particulars of: contracts of employment, certificate of qualifications, changes to terms and conditions	6 years after employment	IL2 – PROTECT
Job history -paper or electronic	6 years	IL0 – UNCLASSIFIED
Current address details	6 years after employment has ended	IL2 – PROTECT
Record of location of overseas service	6 years	IL0 – UNCLASSIFIED
Variation of hours - calculation formula for individual	destroy after use	IL1-PROTECT
Promotion, temporary promotion and/or substitution documentation	6 years	IL1-PROTECT
Working Time Directive opt out forms	3 years after the opt-out has been recinded or has ceased to apply	IL0 – UNCLASSIFIED
Record of previous service dates	6 years	IL0 – UNCLASSIFIED
Previous service supporting dates	6 years	IL0 – UNCLASSIFIED
Qualifications/references	6 years	IL1-PROTECT
Transfer document (OGD E18)	Destroy after summary noted and actioned	IL1-PROTECT
Annual/assessment reports for the last 5 years of service or summary of performance marks where an open reporting system operates	until age 72	IL1-PROTECT
Training history	6 years	IL0 – UNCLASSIFIED
Description	Disposal	Impact level - Protective Marking
Annual leave records (dependent on departmental practice)	2 years	IL0 – UNCLASSIFIED
Job applications - internal	1 year	IL0 – UNCLASSIFIED
Recruitment, appointment and/or promotion board selection papers Interview Notes/Score sheet - unsuccessful candidate	6 months from date created	IL1-PROTECT

Interview Notes/Score sheet - successful candidate	5 years from date created	IL1-PROTECT
Building Society references	6 months	IL0 – UNCLASSIFIED
Health Declaration	6 years	IL1-PROTECT
Health referrals including medical reports from doctors and consultants, correspondence with appointed medical advisor	6 years	IL1-PROTECT
Papers relating to any injury on duty	6 years	IL1-PROTECT
Medical reports of those exposed to a substance hazardous to health, including:	40 years from date at which entry was made	IL1-PROTECT
Lead (control of Lead at work Regulations 1980)	40 years from date at which entry was made	IL1-PROTECT
Asbestos (control of Asbestos at Work regulations 1996)	40 years after last record	IL1-PROTECT
Compressed Air (Work in Compressed Air regulations 1996)	40 years from date of last entry	IL1-PROTECT
Radiation (Ionizing Radiation Regulations 1985)	50 years from date of last entry	IL1-PROTECT
Medical /Self certificates - unrelated to industrial injury	4 years	IL1-PROTECT
Bank details- current	6 years after employment has ended	IL1-PROTECT
Death Benefit Nomination and Revocation Forms	Until age 100	IL1-PROTECT
Death Certificates	Return original copy to provider. Retain until age 100	IL1-PROTECT
Decree Absolutes	6 years	IL1-PROTECT

Description	Disposal	Impact level - Protective Marking
Housing advance	6 years after repayment	IL0-UNCLASSIFIED
Marriage certificate and documentation relating to civil registration	6 years	IL0-UNCLASSIFIED
Unpaid leave periods (maternity leave etc)	Until age 100	IL0-UNCLASSIFIED
Statutory maternity pay documents	3 years	IL1-PROTECT
Other maternity pay documentation	3 years	IL1-PROTECT
Overpayment documentation	6 years after repayment or write-off	IL1-PROTECT
Personal payroll history, including record of pay, performance pay. Overtime pay. Allowances, pay enhancements, other taxable allowances, payment for untaken leave, reduced pay, no pay, maternity leave	until age 100	IL1-PROTECT
Record of: full name and date of birth	6 years after employment has ended	IL1-PROTECT
NI number	6 years after employment has ended	IL1-PROTECT
Pensionable pay at leaving	6 years after employment has ended	IL1-PROTECT
Reckonable service for pension purposes (and actual service where this is different, together with reasons for the difference)	6 years after employment has ended	IL1-PROTECT
Reason for leaving and new employers name (where known)	6 years after employment has ended	IL1-PROTECT
Amount and destination of any transfer value paid	6 years after employment has ended	IL1-PROTECT

Description	Disposal	Impact level - Protective Marking
Amount of any PCSPS contributions	6 years after employment has ended	IL1-PROTECT
Amount and date of any contributions Equivalent premium paid	6 years after employment has ended	IL1-PROTECT
All other papers relating to pensionability not listed above	6 years after employment has ended	IL1-PROTECT
Resignation, termination and/or retirement letters	6 years after employment has ended	IL1-PROTECT
Added years	Until age 100	IL1-PROTECT
Additional voluntary Contributions (AVC)	Until age 100	IL1-PROTECT
Payroll input forms	6 years	IL1-PROTECT
Bonus Nominations	6 years	IL1-PROTECT
Complete sick absence record showing dates and causes of sick leave	Until age 72	IL1-PROTECT
Statutory Sick Pay (SSP) forms	For last 4 to 6 years	IL1-PROTECT
Papers relating to disciplinary action which has resulted in any changes to terms and conditions of service, salary, performance pay or allowances	6 years	IL1-PROTECT
Advances for season tickets, car parking, bicycles, Christmas/holidays or housing	6 years after repayment	IL1-PROTECT

Cafcass Retention Criteria for Corporate/information Management

Description	Disposal	Impact level - Protective Marking
Record keeping		
Diaries	2 years – service user information removed then destroyed	IL2 - PROTECT
FOI requests	3 years after full disclosure	IL1 - PROTECT
FOI – Redacted information or the information requested is not disclosed	10 years	IL2 - PROTECT
Disposal		
Disposal schedules	Retain Permanently	IL2-PROTECT
Lists, certificates, docket books or databases of records destroyed	Retain Permanently	IL2-PROTECT
Copies of catalogues/lists of records transferred to the place of deposit	5 years	IL1-PROTECT
Retrieval of records from the place of deposit	2 years	IL0-UNCLASSIFIED
Storage		
Security of records	5 years	IL2-PROTECT
Records Relating to the use of on-site/off-site storage area	2 years	IL2-PROTECT
Records relating to the transfer of records to on-site/off site storage	2 years	IL0-UNCLASSIFIED
Records relating to the contracts with storage providers	6 years from end of contract	IL1-PROTECT
General Management - Known Best Practice - Companies Act 2006		
Minutes of Board Meetings	Permanent retention	IL0-UNCLASSIFIED
Minutes Signed by the Chair	Permanent retention	IL0-UNCLASSIFIED
Register of seals	Permanent retention	IL2-PROTECT
Register of Board Members	Permanent retention	IL0-UNCLASSIFIED
Register of Board Members interest	Permanent retention	IL0-UNCLASSIFIED
General admin. relating to the provision of information management	2 years	IL0-UNCLASSIFIED
Guides, manuals and instructions on the management of records	Destroy when new issue(s) agreed and circulated	IL0-UNCLASSIFIED
Training records including audiovisual material	5 years	IL0-UNCLASSIFIED

Records

Complaints Records

Known Best Practice - National Archives

Description	Disposal	Impact level - Protective Marking
Policy Statements	When superseded	IL0-UNCLASSIFIED
System handbook/guide	When superseded	IL0-UNCLASSIFIED
Minutes of meetings of Complaints Committee, Service Standards Team, etc	10 years	IL0-UNCLASSIFIED
Surveys	3 years	IL0-UNCLASSIFIED
Case records		
Enquiries	3 years	IL1-PROTECT
Investigations	10 years	IL3 - RESTRICTED
Statistical reports	5 years	IL0-UNCLASSIFIED
Statistical Reports relating to Staff		IL1-PROTECT
Reports on particular complaints or on categories of complaints	3 years	IL3 – RESTRICTED but IL0-UNCLASSIFIED for categories of complaints
Register of Complaints	10 years	IL3 - RESTRICTED
Reviews		
Correspondence and papers	10 years	IL3 - RESTRICTED
Reports	3 years	IL0-UNCLASSIFIED

Procurement

Estates

Known Best Practice National Archives

Description	Disposal	Impact level - Protective Marking
Contractual records – initial proposal		
End user requirement	6 years	IL2-PROTECT
List of approved suppliers	An active document – updated regularly	IL2-PROTECT
Agreed specification	6 years from end of contract	IL2-PROTECT
Invitation to Tender	6 years from end of contract	IL2-PROTECT
Tendering		
Unsuccessful tender documents	1 year after date of last paper	IL2-PROTECT
Successful tender document	6 years from award of contract	IL2-PROTECT
Background information supplied by department	1 year after date of last paper	IL2-PROTECT
Interview panel – report and notes of proceedings	1 year from end of contract	IL2-PROTECT
Commissioning letter	1 year from end of contract	IL2-PROTECT
Signed contract	6 years from end of contract	IL2-PROTECT

Cafcass Retention Criteria for Press & Public Relations Records

Known Best Practice - National Archives

Description	Disposal	Impact level - Protective Marking
Dealing with the media and the public		
Press releases	7 years	IL0-UNCLASSIFIED
Draft press releases	Destroy when superseded	IL2- PROTECT
Press cuttings	1 month	IL0-UNCLASSIFIED
Operational notes (notices to press about forthcoming)	3 months	IL0-UNCLASSIFIED
Draft operational notes	Destroy when superseded	IL2- PROTECT
Press conference reports/previews	3 years	IL0-UNCLASSIFIED
Press reports digests	7 years	IL0-UNCLASSIFIED
Internal records		
Correspondence with branches of the media	7 years	IL0-UNCLASSIFIED
Policy and administrative records	second review (25 years)	IL0-UNCLASSIFIED
Handbooks and guides to media/public	Destroy when superseded	IL0-UNCLASSIFIED
Reports on media/public relations	7 years	IL2 - PROTECT
Image library records	When no longer required	IL0-UNCLASSIFIED
Special events		
Correspondence and papers	7 years	IL2 - PROTECT
Reports	7years	IL2 - PROTECT
Visitor Books	3 years	IL0-UNCLASSIFIED
Calendars	3 years	IL0-UNCLASSIFIED
Brochures and Guides	3 years	IL0-UNCLASSIFIED

Cafcass Retention Criteria for Central Expenditure Records

The disposal period below covers completed year's records (i.e. not including the current year)
 Known Best Practice - National Archives

Description	Disposal	Impact level - Protective Marking
Estimated records (including revises and supplementary) where detailed justification is provided and which are submitted to the Treasury	6 Years	IL0-UNCLASSIFIED
Estimates submissions from regional or local offices	2 years	IL0-UNCLASSIFIED
Calculations and costings for annual estimates	2 years	IL0-UNCLASSIFIED
Expenditure scrutinies	2 years	IL0-UNCLASSIFIED
Records relating to bids from the contingencies fund	6 Years	IL1-PROTECT
Spending reviews	1 year after the cycle to which the records relate	IL0-UNCLASSIFIED
Records relating to dealings with the public accounts committee an the select Committee on expenditure	6 years	IL1-PROTECT
Expenditure and revenue returns	1 year after the year to which the returns relate	IL0-UNCLASSIFIED
Financial statements prepared for annual reports	1 year after publication of the report	IL0-UNCLASSIFIED
Financial statements prepared for management	1 year after completion of annual financial report	IL1 - PROTECT
Grant funding records	6 years after action completed/grant made	IL0-UNCLASSIFIED
Financial authorities or delegations	6 years after authority or delegation is superseded	IL1 - PROTECT

Cafcass Retention Criteria for Accounting Records

All retention periods are given in whole years and should be calculated from the end of the financial year to which the records relate. The retention periods cited are based in the General NAO requirements.

Description	Disposal	Impact level - Protective Marking
Cheques & associated records		
Cheque book/butts for all accounts	2 years	IL2 - PROTECT
Cancelled cheques	2 years	IL2 - PROTECT
Dishonored cheques	2 years	IL2 - PROTECT
Fresh Cheques	6 years	IL2 - PROTECT
Paid/presented cheques	6 years	IL2 - PROTECT
Stoppage of cheque payment notices	2 years	IL2 - PROTECT
Record of cheques opened books	2 years	IL2 - PROTECT
Cheque registers	2 years	IL2 - PROTECT
Record of cheques drawn for payment	6 years	IL2 - PROTECT
Bank deposits		
Bank deposit books/slips/butts	2 years	IL2 - PROTECT
Bank deposit summary sheets: summaries of daily banking: cheque schedules	2 years	IL2 - PROTECT
Register of cheques lodged for collection	2 years	IL2 - PROTECT
Bank reconciliations		
Reconciliation files/sheets	2 years	IL2 - PROTECT
Daily list of paid cheques	2 years	IL2 - PROTECT
Unpaid cheque record	2 years	IL2 - PROTECT
Bank Statements		
Bank statements, periodic reconciliations	2 years	IL2 - PROTECT IL2 - PROTECT

Description	Disposal	Impact level - Protective Marking
Bank certificates of balance	2 years	IL2 - PROTECT
Electronic Banking and electronic funds transfer		
Cash transactions; payment instructions; deposits; withdrawals	Disposal action inline with paper records	IL2 - PROTECT
Audit trails	Retain for the same period as the base transaction record.	IL2 - PROTECT

Health & Safety

Known Best Practice - Health & Safety at Work Act 1974

Description	Disposal	Impact level - Protective Marking
Young Persons Risk assessment	Discarded on the person reaching 21 Years of age	IL1-PROTECT
Risk Assessments	Discarded when the risk assessment is no longer considered valid	IL1-PROTECT
Accident & Incident form	3 years	IL1-PROTECT
Accident & Incident book (BI 510)	3 years following the last entry in the book	IL1-PROTECT
Records of Asbestos surveys	Life of building – handed over to new tenants/landlord where applicable	IL1-PROTECT
Health and safety file for occupancy of new buildings generated by the CDM coordinator	Life of building – handed over to new tenants/landlord where applicable	IL1-PROTECT

INFORMATION ASSURANCE POLICY

Appendix 2

Appendices	
1	Retention & Disposal Practice
2	Protective Marking Schedule
3	Keeping Desks Clear of Confidential Material Policy
4	Cafcass Premises Security Procedures
5	Managing Emails Guidance
6	Reporting Data Breaches

Appendix 2 Protective Marking Guidance

These markings can be applied to any government assets, although they are most commonly applied to information held electronically or in paper documents.

Note that the classification must be placed in the header of each page of each document (this will be prompted on the Flex system).

Classification	Control	Transportation	Disposal
UNCLASSIFIED	All documents that are not classified as 'Protect; Restricted; Confidential' should be marked 'Unclassified'.		
PROTECT	<p>This document is for internal use only. Access to this information is confined to Cafcass employees and associated service users and service providers (Personal data can be shared with the persons to whom it relates to and in Cafcass' case parts will be for restricted circulation as per court rules).</p> <p>The Protect marking is used to cover public finances, the provision of a service, reputation, and safety of citizens. Access to Restricted material should be limited to staff who have been cleared to process them. Staff should also implement the need to know principle to prevent unauthorised access or disclosure.</p>	<p>Documents should only be transported as necessary. The preferred format for Restricted documents is electronic. Efforts should be made to store documents securely wherever possible.</p> <p>If paper copies must be transported, they should be contained in a folder marked as "PROTECT" and in briefcase or bag.</p> <p>(Where only a few of the documents on a file have a protective marking, you should consider whether it is necessary to keep the whole file secure or whether you could remove the protected documents and keep them secure separate from the main file.)</p> <p>Documents should not be left unattended in public areas or vehicles at any time.</p> <p>If information is held on a laptop then this must be encrypted.</p>	<p>Cafcass will carry out electronic disposal of documents and archiving.</p> <p>The disposal of Protected paper documents will be carried out in accordance with the Information Assurance Policy and will be an administrative task. Individual practitioners must not destroy documents –this includes handwritten notes.</p> <p>Methods of destruction must include the destruction of the information contained within the document. This may be achieved through shredding or incineration.</p>

<p>RESTRICTED</p>	<p>This document is for internal use only. Access to this information is confined to Cafcass employees and associated service users and service providers. (Personal data can be shared with the persons to whom it relates to and in Cafcass' case parts will be for restricted circulation as per court rules.) Disclosure of such information must also accord with relevant court rules.</p> <p>The Restricted marking is used to cover the vast majority of Cafcass case files work including most Casework and Personnel files. Access to Restricted material should be limited to staff who have been cleared to process them (CRB checked or in accordance with Business Area policy). Staff should also implement the need to know principle to prevent unauthorised access or disclosure.</p> <p>Consent from a senior manager is required to release this information in any other circumstances. If documentation needs to be used outside of Cafcass Office environment, the documentation must be kept secure, must not be viewed in public areas (eg on public transport or court waiting areas).</p> <p>When not being directly used paper copies must be kept in locked drawers or briefcases.</p>	<p>Documents should only be transported as necessary. The preferred format for Restricted documents is electronic. Efforts should be made to store documents securely wherever possible.</p> <p>If paper copies must be transported, they should be contained in a folder marked as "RESTRICTED" and in briefcase or bag.</p> <p>(Where only a few of the documents on a file have a protective marking, you should consider whether it is necessary to keep the whole file secure or whether you could remove the protected documents and keep them secure separate from the main file.)</p> <p>Documents should not be left unattended in public areas or vehicles at any time.</p> <p>If information is held on a laptop then this must be encrypted.</p>	<p>Cafcass will carry out electronic disposal of documents and archiving.</p> <p>The disposal of Restricted paper documents will be a carried out in accordance with the Information Assurance Policy and will be a Business Support task. Individual practitioners must not destroy documents –this includes handwritten notes.</p> <p>Methods of destruction must include the destruction of the information contained within the document. This may be achieved through shredding or incineration.</p>
<p>CONFIDENTIAL AND HIGHER CLASSIFICATIONS</p>	<p>Documents should be kept in security containers offering adequate protection, their whereabouts recorded and maintained in a register which should be maintained centrally or with each Office.</p>	<p>Documents should only be transported as necessary and with the consent of a senior manager.</p>	<p>Cafcass will carry out electronic disposal of documents and archiving.</p> <p>The disposal of Confidential and higher classification paper documents will be a carried out in accordance with the Information Assurance Policy and will be a Business Support task. Individual practitioners must not destroy documents –this includes handwritten notes.</p> <p>Methods of destruction must include the destruction of the information contained within the document. This may be achieved through shredding or incineration.</p>

INFORMATION ASSURANCE POLICY

Appendix 3

Appendices	
1	Retention & Disposal Practice
2	Protective Marking Schedule
3	Desk of Confidential Material Policy
4	Cafcass Premises Security Procedures
5	Managing Emails Guidance
6	Reporting Data Breaches

Appendix 3 Desk Clear of Confidential Material Policy

1 Objective:

- 1.1 The objective of the this policy is to put in place measures which will help to reduce the risk of security breaches, fraud and information theft caused by documents being left unattended in Cafcass premises.

2 Background:

- 2.1 All Government Departments and their NDPBs are required to safeguard information of a personal or confidential nature that it holds on employees and service users.
- 2.2 There have been some well-publicised breaches relating to loss of electronic records but paper records are equally important and must be kept in secure conditions. The introduction of this policy assists this objective in the following ways:
 1. It reduces the threat of a security breach and information theft as confidential information is locked away
 2. It ensures compliance with Data Protection regulations by keeping personal data secure.
 3. It reduces the chance of identity theft.
 4. It demonstrates that Cafcass is taking corporate responsibility for the personal data it processes.
 5. It is generally accepted that a tidy desk is a sign of efficiency and effectiveness and reduces the risk of losing confidential documents.

Scope

- 2.3 This policy applies to all permanent, temporary or contracted staff employed by Cafcass, and to all students and volunteers who can access information. Staff are required to comply with the policy and managers and supervisors must monitor compliance on a regular basis. Failure to comply will be regarded as a disciplinary incident and will be dealt with under the Performance and Conduct Policy.

3 The Policy in Operation

- 3.3 The day-to-day implementation of the policy is very easy to apply. At the end of the working day or when leaving the office for a major part of the day, all staff must remove and lock away any papers and files with personal information in them. Cafcass provides appropriate lockable under desk lockers and filing cabinets for this purpose. All filing cabinets and any other drawer or storage cupboard containing personal data of any kind

must be locked over night. This includes business cards, lists containing private phone numbers and all pieces of paper with any personal data on it.

- 3.4 Staff are encouraged to think carefully whether they need to print out information containing personal data and to dispose of it securely when it is no longer needed. This both reduces the amount of paper used and reduces the risk of it being lost or falling in to the wrong hands.

5 Corporate responsibility

- 5.1 The Senior Information Risk Owner (SIRO) has ultimate responsibility for ensuring compliance with this policy. All staff have responsibility for reporting information security incidents/breaches to their line manager and to the Information Assurance & Data Handling Officer.
- 5.2 All staff are required to comply with this policy and where requested, to demonstrate such compliance.

6 Tips for having a tidy desk

- Put a date and time in your diary to clear your paperwork
- If in doubt - throw it out. If you are unsure of whether a piece of paper should be kept - it will probably be better to put it in the secure waste disposal.
- Always use secure recycling bins for office paper no longer needed.
- Do not print off emails to read them. This just generates increased amounts of clutter
- Go through the things on your desk to make sure you need them and what you don't need throw away.
- Handle any piece of paper only once - act on it, file it, or put it in the bin.
- Always clear your desktop before you go home

INFORMATION ASSURANCE POLICY

Appendix 4

Appendices	
1	Retention & Disposal Practice
2	Protective Marking Schedule
3	Desk Clear of Confidential Material Policy
4	Cafcass Premises Security Procedures
5	Managing Emails Guidance
6	Reporting Data Breaches

Appendix 4 Cafcass Premises Security Procedures

1 Objective

To set out the physical security measures within Cafcass premises to be followed to help reduce the risk of security breaches, fraud and information theft.

2 Background

There are potential risks to security given the sensitive personal information that is held within offices. These procedures set out the responsibilities of all staff when controlling this risk. GSI (Government Secure intranet) also provides for the protection of data held within Cafcass data. Information on providing for personal safety on Cafcass premises is contained within the Personal Safety Policy (for further information contact the National Health and Safety Co-ordinator).

3 The Policy in Operation:

Cafcass requires all offices via the Office Manager to:

- Hold a list of all staff that access the building.
- Insist staff wear ID badges.
- Provide temporary ID passes to visitors in the building.
- Insist all desks are clear of personal identifiable data on a daily basis.
- Complete an [induction checklist](#) and also convey the importance of security of the building.
- Be protected by an alarm system when building is not occupied.
- Have lockable internal access systems e.g. Keypad, swipe cards. Keypad codes must be changed on a regular basis.
- Use lockable cabinets to store all personal and financial information.
- Keep cabinets in areas where there is no public access.
- All communications equipments cabinets should be locked and away from public access. (i.e. no cleaning/storage equipment to be housed in the Communications Cabinets).
- Keys need to be managed to ensure that only those persons who are authorised can obtain them and gain access to valuable information assets.
- Use a key safe with a combination lock or digital locking mechanism.

Cafcass requires all staff to:

- Implement the Cafcass Keeping Desk Clear of Confidential Information policy.
- Make sure that all keys be locked away in a key safe when not in use.
- Inform Office Managers when keys are lost.
- Wear ID badges at all times.
- Be aware of and adhere to the [Personal Safety](#) policy.
- Use of lockable cabinets / rooms to store files which contain any personal data.
- All staff understand 'Line Management' e.g. When anything needs to be reported they understand whom to contact.
- Make sure all personal information is not visible by members of the public.
- Understand accept the relevant policies and procedures outlined in the Information Assurance policy.

Appendix 5

Appendices	
1	Retention & Disposal Practice
2	Protective Marking Schedule
3	Keeping Desks Clear of Confidential Material Policy
4	Cafcass Premises Security Procedures
5	Managing Emails Guidance
6	Reporting Data Breaches

Appendix 5 Managing your emails

1 Introduction

Emails should be treated in the same way as you would treat any other form of recorded communication. In many instances emails will form part of our corporate record, or a case record. This guidance is designed to help you manage your emails. It is consistent with other related Cafcass policy (the Information Assurance policy, the IT Security policy and the Case Recording policy). You need to make sure you have read and understood these policies before viewing the guidance.

Effectively managing your emails will help you to:

- Comply with Cafcass policy;
- Ensure that you can find what you want when you need it (including when requested from the court);
- Ensure that your colleagues can find important information even if you are not in the office;
- Ensures that you inbox does not get full and then stop you being able to send and receive emails;
- Assist with compliance with the Data Protection Act 1998 and the Freedom of Information Act 2000.

2 What issues should I consider when composing emails?

Remember that your email message may be disclosed in response to an information request under the Freedom of Information 2000, the Data Protection Act 1998 or as part of a court case. Avoid using email to let off steam, including by copying the email to a large number of people. Ensure you read it before sending it, and check:

- Does it say what you want it to say?
- Is the tone of the email as you intended?
- If it were a memo or formal letter, would you write it in the same way?
- Do you need to send it to all the people to whom it is addressed?

3 What issues should I bear in mind when writing email about an individual?

As well giving people the right to see the information we hold about them, the Data Protection Act also requires us to ensure that the information we hold about identifiable, living individuals is relevant and accurate but not excessive. The following points will help you to achieve this in your emails:

- Do not include irrelevant information;
- Clearly differentiate between matters of fact and opinion;
- Do not express opinions that you are not prepared to defend, or which you cannot substantiate;
- Do not express opinions in areas where you are not qualified;
- Always be sure of the facts; and
- Do not write in anger or in haste.

4 What should I consider when sending an attachment(s)?

If the attachment contains information that can be accessed via shared folders, a shared drive or an internal or external Cafcass website, provide a link to the document rather than attaching it to the email.

Whether you provide a link or attach the original document, please bear in mind the need to ensure that everyone can read it (that they have the right program available to them). In general, it is also worth double checking attachments against the questions in the above sections to be sure that you are circulating relevant and appropriate material to the right people.

5 What emails should I keep or delete?

Emails should be treated in the same way as you would treat any other form of recorded communication. Whenever an email is sent or received a decision should be made about whether the e-mail needs to be kept as a record. See Section 1 of the Information Assurance policy for what constitutes a record. Section 3 and Appendix 1 of the Information Assurance Policy for further detail on how long a record must be kept for. Emails can also form part of the case record; see Section 8 of the case recording policy for the retention of case records.

In addition to what is contained within the policies, you should consider the following when determining whether to save an email:

- **If there is a legal requirement to keep the information;**
- **If we need the information to carry out our business, such as day-to-day administrative records or material potentially relevant to present or future research;**
- **If we need the information for financial purposes;**
- **If we may need the information to explain why we arrived at a particular decision;**
- **If we may need the information if our decision is challenged in court;**
- **If we may need the information to be publicly accountable for our policies and decisions;**
- **If we may need the information to help us deal with similar situations in the future, such as records that show what procedure was followed in a particular situation or copies of past references provided for students or staff;**
- **If we may need the information to defend our rights and responsibilities, or the rights and responsibilities of others; or**
- **The information has value for historical research purposes.**

As well as the text of the email, it is important to keep the associated metadata (data about the data) about the email, such as to, from, date, time, and subject. This is necessary to understand the email and can affect the credibility a court will give to email evidence.

Unless the email has been received from an external correspondent, it is the responsibility of the sender of an email to decide whether or not to save the email. This is because each message has only one sender but may have many recipients. When you send an email, unless you have altered your settings, a copy will be saved

automatically in the 'sent items' folder. As you will periodically clear this folder to manage your storage limit a 'sent items' folder should be created in your archive in order to move across items which need to be retained. Alternatively, you can export a copy of an email to a case or other network folder so that emails can be retained with other case information (use the 'file, save as' function).

When dealing with long email strings, provided that the string has not been edited and all the previous emails are part of the string, it is sufficient to keep the last email in the string and to destroy the others.

6 For how long should I keep my e-mails?

The retention period of email is determined by its content. Retention decisions have to be taken on a case-by-case basis at the time of receiving or sending email based on Section 3 and Appendix 1 of the IA policy.

If you make arrangements to place those emails which need to be saved as a record somewhere other than your in box and sent items folder (i.e. kept in the shared drive), the remaining emails can be destroyed after a very short period.

7 Where should I store emails?

Decide whether to leave the message in its present folder, to delete it immediately or to move it elsewhere. Keeping it in your sent items folder or inbox means that it is inaccessible to others that might need it and can make it difficult to retrieve information once the folder becomes too large. For business continuity purposes, and also to enable Cafcass to meet its FOI and DP obligations, emails which form part of the corporate record should be stored where they will be accessible to other staff in your area as well as to yourself.

If, based on the Information Assurance policy you think an email kept as a permanent record, this should be saved, ideally as a plain text document, on the shared server in a relevant folder.

Some emails do not need to be kept beyond the time frame of the task to which they refer. A simple way to deal with this is to move them to a temporary network folder named after the task to which they refer. Once the task is complete, the whole folder can be deleted.

This has the advantages of:

- Electronic records on a particular topic all kept together, regardless of original format;
- Being accessible to everyone that needs to see them; and
- Making it easy to search content of a range of records in different formats to find the relevant information.

Some emails may also need to be included on the case file. For further detail see the Case Recording Policy.

8 How should I go about clearing out unwanted emails?

Delete unnecessary or out-of-date emails as soon as they are no longer required, as having too many emails can become difficult to manage. Some ways of doing this include:

- sorting by date and deleting all those over a certain age;
- sorting by addressee/sender and deleting all those sent to or received from certain individuals;
- sorting by subject and deleting those relating to completed business; and
- sorting by size and deleting large e-mails that are no longer required.

However you must consider whether any of these emails need to be kept as part of the case or corporate record, and save these in the shared drive or server before deleting.

9 What should I do about my emails when I am away from the office?

The deadline for responding to Freedom of Information and Data Protection requests is calculated from the date that Cafcass received a request for information, and not from the date that you read it.

If you are out of the office and unable to check your email for more than a week, you should set an out of office message that provides an alternative contact point for the time you are away.

If you work in a high-profile role, or one that regularly generates enquiries that could be viewed as freedom of information requests, a sensible approach is to set an out of office message and also to arrange for your emails to be checked in your absence. This should always be through the use of the delegation tools in Outlook and never by sharing your username and password with another staff member.

If you are responsible for managing a shared email account then it is also important that you ensure there is cover for this whilst you are away from work.

10 What should I do if a member of my staff is unexpectedly away from the office, for example, on long-term sick leave?

As soon as it becomes apparent that the member of staff will be away for a long period of time, or once the person has been absent for a week with no prospect of return, you should ask your IT support service to set an out of office message providing alternative contact details. Delegation can also be set up to a suitably authorised alternative contact.

11 What security issues should I consider?

All emails may be monitored by Cafcass to ensure correct usage. Emails are not private or confidential and can be legally intercepted. It is the responsibility of all members of staff to consider the appropriateness of using email to discuss sensitive subjects. Highly sensitive information should not be sent by ordinary email. Remember that whilst an email may be sent to an individual's account (s)he might not be the only person who sees it. Make sure you have read and understood the Cafcass IT Security Policy. When dealing with staff from other organisations you should also

ensure that they are using secure facilities, such as CJSM email accounts, rather than personal accounts.

12 I sometimes send and receive work emails from a personal email account. What issues should I consider?

You should not send, receive or forward work emails to a personal email address. Cafcass provides all employees with a secure email address and that is the only email address that can be used for Cafcass business.

What help is available?

IT Support (helpdesk)
IT Client Services Manager
Information Assurance & Data Handling Officer
Cafcass Legal.

INFORMATION ASSURANCE POLICY

Appendix 6

Appendices	
1	Retention & Disposal Practice
2	Protective Marking Schedule
3	Keeping Desks Clear of Confidential Material Policy
4	Cafcass Premises Security Procedures
5	Managing E-mails Guidance
6	Reporting Data Breaches – See PDF on g-drive