Cafcass Case Recording and Retention Policy

Overview of Policy

This policy sets out the requirements placed by Cafcass on its staff and contractors relating to case recording and retention.

1.0 Introduction

1.1 This policy includes:

- the requirements for case recording, using Cafcass' Electronic Case Management System (ECMS);[1]
- the requirements for maintaining the security of information; and
- the roles and responsibilities for the creation, maintenance, access, storage, closure and destruction of case records.

1.2 This policy must be complied with by everyone who is working for Cafcass, including on a contracted basis, unless there are exceptional reasons which justify a variation. In such situations a clear explanation must be provided in the electronic case file, and a manager notified as soon as possible.

1.3 This policy should be read in conjunction with the Cafcass Reporting to Court policy, for expectations in relation to the sharing of records and transparency of case recording and reporting.

2.0 The case record

2.1 The case record is held on ECMS, consisting of the folders set out in the Appendix. Where two Guardians are appointed in the same case, there will be two separate case files on ECMS.

2.2 Practitioners are responsible for:

- ensuring that case recording in ECMS creates a comprehensive and consistent case record, with information recorded contemporaneously[2] whenever appropriate;
- updating ECMS with information pertaining to their allocated cases, including the recording of relevant diversity information,[3] and that information in all cases and all law types (e.g. hearing dates, filing dates) is accurate and complete;
- Clearly marking on the case file any information (including addresses) that is confidential, specifying who it can and cannot be shared with;
- ensuring that all relevant actions on cases relating to their analysis, planning and intervention are contemporaneously recorded on ECMS;

---

[1] Information for staff on using ECMS, including contact details of ECMS admin staff, is available on the intranet

[2] For the purposes of case recording in Cafcass, contemporaneous recordings means those made either at the time of the event, or so shortly afterwards that the facts are fresh in the memory of the author. For the purposes of this policy this must be within three working days of the event.

[3] See diversity guidance.

- ensuring that relevant information received by them from individuals or agencies external to Cafcass is scanned and saved onto ECMS;
- setting up the Outlook auto-forwarding rule to forward ECMS alert notifications to the locally agreed business support mailbox, when out of the office; and
- setting up an auto-forward for business support staff, so that business support staff are alerted to incoming correspondence.

2.3 Office Managers are responsible for:

- having systems in place so that all case related communication and information processed by Cafcass is recorded in the contact log by the recipient and, within one working day, scanned to ECMS. This includes information received from any source (e.g. telephone message, letter or personal caller) with date, time, information or message and any action required, to alert the practitioner or manager responsible; and
- arranging for items belonging to service users, in the care of Cafcass as part of indirect contact arrangements, to be stored securely on Cafcass premises.

2.4 The Service Manager is responsible for:

- ensuring there is a duty system in place so that information from any source is recorded on the contact log by its recipient, and that the SM or allocated practitioner is alerted;
- ensuring the correct allocation of work in ECMS;
- overseeing quality of casework, decisions and case closure in ECMS;
- entering on the case record: case-related information prior to allocation; case related actions arising from supervision or complaints; case-related information if the practitioner has an extended absence from work;
- ensuring that the approval process is carried out in ECMS for each report or letter filed. Only FCAs having been assessed to 'self-file' by the Service Manager within iTrent have the permission to opt to self-approve in ECMS. All other reports should be approved by an Enhanced Practitioner or Service Manager;
- not approving any report where any changes are needed to bring it up to a good standard; and
- ensuring that the approver does not make track changes or amendments to the report; any changes required should be noted using the Microsoft Word 'Comments' facility or, if extensive, in an attached Word document or QA tool.

2.5 Paper court bundles are not to be scanned or saved to ECMS. They are to be kept in paper form throughout the life of the case and shredded at the point of case closure. When documents that make up the court bundle are received electronically and saved to ECMS, there is not a requirement that these documents are deleted from ECMS at the end of the case, with the exception of police information (see Section 11). When electronic bundles are received by email they should not be uploaded to ECMS, as they can be filed in and accessed from Outlook archives or in the H drive. These locally stored documents must be deleted at the end of the case by the practitioner, and they do not need to be transferred to ECMS.

2.6 A paper file will only ever be created and held to store documents that cannot be scanned (for example a child's drawing that is too large to be scanned). Most documents can be scanned and originals returned to source or destroyed, once the quality of the scan has been checked.

2.7 In private law cases the Central Intake Team will set up the file on ECMS and will be responsible for transferring cases to local teams when the screening stage is complete. In public law cases this is done locally. ECMS is organised into separate sections as set out in the Appendix.

3.0 Self Employed Contractors and ECMS

3.1 When a case is allocated to a Self Employed Contractor (SEC) the case will also be created in ECMS. SECs are required to ensure all their case work is completed on Cafcass current templates (case plan and reports), with the exception of the completion of the electronic contact log. SECs must submit a completed activity log which can serve the same purpose as a contact log as it includes all relevant data to enable business support to update ECMS.

4.0 Security of information in all cases

4.1 Documents saved to ECMS must follow this standard file naming convention: case name, Cafcass case number, document name.

4.2 Reports must be filed as PDF files, and the filed version saved as a PDF in ECMS, so that the document can no longer be amended. The date on which a report is filed at court must be recorded in the contact log. Any earlier draft version(s) should be deleted from ECMS at the point at which finalised reports are saved as a PDF and filed, with the exception of one Word version of the court report, to allow for future submissions that require additions to the original. When sending the report for approval, it is automatically created into a PDF on approval. On initiating the process, FCAs must not tick the box to delete the Word document.

4.3 Any other documents to be sent externally, including letters, must be saved as a PDF file prior to emailing so that they cannot be amended and so that track changes cannot be viewed by the recipient. Any email correspondence sent externally, for example by Business Support to the court when filing a report, must also be uploaded and saved to ECMS correspondence section.

4.4 Third party paper documents that are scanned to ECMS as part of the case record (e.g. a child's drawing, correspondence from third parties) must be scanned and saved to ECMS within seven days of receipt of the document by Cafcass. The scanned image must be checked for legibility and the original then destroyed or returned to source (as deemed appropriate by the FCA).

4.5 If a paper file is necessary for items that cannot be scanned, the items must be stored in locked cabinets when not being actively worked on, and a record of the location completed in the contact log. No case-related information may be left unsecured. Workstations must be cleared of case-related material when the worker using the material completes the work or leaves the office for more than a brief period. Any member of staff finding unsecured case-related information must take action to secure it.[4]

[4] See the Cafcass Information Assurance Policy for more detailed guidance about the security of all (i.e. not just case related) information.

4.6 Hard copies of Cafcass case related documents containing personal/sensitive personal information (e.g. safeguarding letters and court reports) should not be printed or removed from Cafcass offices (including home-based offices). All documents contained within ECMS can be accessed and worked on offline and should not be printed from ECMS for reference. Court bundles received in paper form from local authorities should be used throughout the life of the case and shredded at case closure (see paragraph 2.5). In situations where staff or SECs must carry case-related paper information away from its secure base all necessary steps must be taken to ensure its location is known at all times, its security and later destruction.[5]

4.7 The printing of personal/sensitive personal information provided by third parties (e.g. police, health bodies and local authorities) about service users is prohibited in all circumstances.

4.8 All Cafcass case related data is at the security classification level OFFICIAL and will usually contain sensitive personal information of service users. It therefore needs to be sent securely when it is shared or transferred to avoid unauthorised disclosure, which could breach the Data Protection Act 1998 and the Family Procedure Rules 2010. For guidance on how to share and transfer case related data by post or by email please refer to **appendix 3.**

4.9 When case-related paper information is being moved between offices, the office managers at the initiating and receiving office must be informed so that the movement of the file can be tracked. The office that sends the document or file retains responsibility for the file until it is signed for by the receiving office.

4.10 The receiving office must be informed, by the initiating office, of the expected arrival time of case-related paper information. Its receipt must be confirmed by email and its location recorded in ECMS.

4.11 Neither paper documents nor the case-related data that is stored on a laptop or other electronic device are to be left unattended, for example in a car, on public transport or in any other public place. Laptops and tablets should always be locked when not in use. The person responsible for the information should know its location at all times.

4.12 When ECMS is accessed offline away from a Cafcass office e.g. in court or at home, the practitioner is responsible for its safety. The screen must be kept out of view of others to ensure the information is kept safe.

4.13 The case record may only be accessed for the purposes of case work (such as quality assurance) including recording case-related messages; and for research or other corporate reporting needs (e.g. aggregation for inspections, reports for Ministers).

4.14 When a case needs to be sealed for a Serious Case Review, an electronic copy of the file must be taken immediately by the Head of Service and saved outside ECMS in a zipped file, with the date copied in the file name. This will serve as the 'sealed' record of the case at that point in time.

[5] This requirement applies irrespective of employment status or work-base. For those who are home-based, the secure base will be the home office rather than a Cafcass office.

5.0 Shielding cases in ECMS

5.1 In some high risk cases that meet the criteria set out in paragraph 5.2 it may be necessary to hide, by shielding, all case related information held by Cafcass to prevent sharing information that could increase the risk of harm to a child, adult, staff member or SEC.

5.2 A decision to shield a case may only be taken by a Head of Service following a recommendation made by an FCA and supported by a Service Manager. Once this decision has been made it is for the Service Manager to decide who should have access to the case information once it has been shielded (i.e. FCA/BS/SM/Cafcass lawyer). Shielding decisions will be made on a case by case basis, at any point during the case, to prevent the following:

- placing a child at risk of a serious incident;
- putting a child's adoption/placement at risk;
- placing an adult at risk of a serious incident;
- prejudicing the prevention or detection of a serious crime;
- risk to staff or SECs; or
- prejudicing a high profile case.[6]

5.3 The FCA is responsible (with assistance from Business Support) for locating and shielding case related information (including any associated closed cases) on all case recording systems: ECMS, ECF Archive, CMS retrieval and G drive. Please see **appendix 2** to view a step by step checklist to be followed when shielding cases.

5.4 Examples of when an individual (and therefore any relevant cases) could be shielded are:

- A child's placement or location is to remain secret and there are perceived risks to this information being elicited by deceit or threat;
- There is a court order preventing the disclosure of the child and/or their parent/carer's whereabouts and there is a perceived risk of this being elicited by deceit or threat;
- A child and/or their parent/carer or family member are subject to witness protection;
- To protect the well-being of children and their adult family members where there is a high risk of publicity, causing distress, should the security of the system be breached;
- When there may be a risk to an allocated worker or other member of staff working on the case if their name is known;
- Staff members are themselves a party to proceedings; or
- The need to shield may also arise in a very limited number of unique circumstances not covered by the above categories, such as siblings of children in the above categories, and all should be assessed on a case-by-case basis.

NB. A confidentiality request on the C100 alone does not of itself warrant a shield request unless reinforced by one of the above categories.

[6] Cafcass' Corporate Management Team will be alerted to any case that is shielded due to high profile or likely media interest.

6.0 Secure emails

6.1 Cafcass operates on the Government Secure Intranet platform (GSI). Cafcass staff are not authorised to send protected information to agencies and service users via non-secure email. Cafcass staff must use Egress Switch to send case-related information to agencies and service users where secure email is not available. No case-related material must ever be sent to a staff member's personal/non-Cafcass email address (for further information about email security, refer to the Information Assurance Policy).

6.2 When receiving case-related information via email, staff must ensure that agencies and professionals working with us understand that sending emails to GSI is secure, and they are not required to password protect documents. More information on Egress Switch is available on the Cafcass website for Egress email recipients and SECs, and on the Intranet for Cafcass staff.

6.3 System generated emails are optional at different points within a case, for example to inform:

- Local authority of closure of a case;
- Court of allocation or closure of a case and appointment of a solicitor; or
- Solicitor of closure of a case.

Check boxes are to be selected when the generated emails are appropriate and are automatically sent to the agency email addresses stored in the database.

7.0 Monitoring Case Record

7.1 The Service Manager is responsible for:

- reviewing management information reports and data compliance reports on a regular basis to ensure that data is accurate and complete in all cases;
- regularly reviewing the quality of case recording and case planning, and recording this in the case plan at appropriate intervals; case plan reviews are due appear in the Service Manager ECMS dashboard;
- accessing reports for quality assurance (QA) as required under the QA Framework from ECMS and recording in the contact log when QA has taken place. QA tools must be completed and logged in iTrent unless the reviewing of a report is through the ECMS approval process;
- Approving reports through the ECMS approval process (section 2.4) and recording points for improvement or amendment appropriately; and
- reviewing cases for closure within ECMS and recording the closure authorisation within the electronic case plan, prior to changing the case status to closed.

7.2 The Office Manager is responsible for:

- the oversight of team data quality and integrity on ECMS;
- reviewing management information reports and data compliance reports on a monthly basis to ensure that data is accurate and complete in all cases.

7.3 The National Improvement Service Managers are responsible for:

- when requested or when appropriate, completing QA tools within iTrent;
- undertaking the approval process in ECMS when requested;

- periodic audits of ECMS information and reporting any recommendations for action to the Head of Service/Assistant Director, as commissioned by the National Service Director; and
- undertaking regular audits of business support responsibilities, ECMS accuracy and data integrity, as commissioned or agreed within internal audit schedules.

7.4 The Cafcass National Service Director, as 'Information Asset Owner' in respect of case records, is responsible for:

- carrying ultimate responsibility for the quality and security of case related information throughout Cafcass' operational areas; and
- commissioning periodic audits to monitor the quality of case recording and compliance with this policy.

7.5 The Heads of Service and Assistant Directors are responsible for:

- implementation of this policy and any associated guidance that may from time to time be issued within their area;
- ensuring that Service Managers monitor case recording as set out above, and recording this in the performance management system;
- ensuring that management information data compliance is achieved to reflect accurate performance information in each service area; and
- undertaking periodic audits to monitor the quality of case recording and compliance with this policy.

8.0 The Case Plan

8.1 The purpose of the case plan is to set out the planning, reflection, analysis and review that is undertaken throughout the life of the case.

8.2 The case plan must be commenced in private law upon Cafcass being directed to undertake work after first hearing, and at the initiation of Cafcass' involvement in public law. It is to be updated at stages relevant to developments in the individual case.

9.0 Case Closure

9.1 For both private and public law cases, employed practitioners may close their own cases when they have been assessed by their Service Manager as having authority to do so, providing that assessment is recorded within their iTrent supervision record.

9.2 Where employed practitioners do not have authority to close cases, they must inform their Service Manager by email when the case is ready for closure in ECMS, to enable closure to be completed by the Service Manager within the timescales set out below. The cases due for closure will appear in the Service Manager ECMS dashboard.

9.3 At the end of SEC cases and at the point of closure, the SEC must email all case documents via secure email to Cafcass business support. When receipt is confirmed, all case information must be securely deleted from the SEC's hard drive. Business Support will upload the documents to ECMS and inform the Service Manager that the case is ready to be reviewed and closed.

9.4 Private Law Cases:

A Work to First Hearing case is closed when:

- the FHDRA outcomes form is completed by the practitioner with confirmation of the outcome of the first hearing, and that the case is ready for closure. Outcomes are to be submitted by the end of the working day following the hearing. In some circumstances, the final legal outcome may be obtained by teams rather than the practitioner, and it may be necessary to record an 'unknown legal outcome' in certain cases; and
- safeguarding checks have been completed, or it is recorded on the case file that checks are not required; and
- the outcome is recorded by the FCA or a member of Business support; and
- the case is registered as closed on ECMS.

A Work after First Hearing case is closed when:

- the outcome section of the case plan is completed, either with final legal outcome or 'unknown legal outcome'; and
- there are no future hearings for Cafcass; and
- it is authorised for closure via the local management process; and
- the outcome is recorded, or logged as unknown; and
- the case is registered as closed on ECMS.

9.5 The allocated practitioner must complete the case closure section of the case plan (except in WTFH cases), and inform the Service Manager that the case is ready for closure in ECMS (or self-close if applicable) no later than two weeks from the point that Cafcass has no further work to undertake (that is, the hearing date). There is no expectation to upload an order received on a closed case, unless this is an order for further work to be completed by Cafcass.

9.6 Public Law Cases:

9.7 The allocated practitioner must complete the case closure section of the case plan and inform the Service Manager the case is ready for closure (or self-close if applicable), within four weeks of the final hearing date.

9.8 If the practitioner was not present at the final hearing s/he is responsible for ascertaining the outcome and for undertaking any final work that may be needed with the child, other family members, the Independent Reviewing Officer (IRO) or other local authority staff. This includes formal handover to the IRO as per the national joint protocol.

9.9 The case may be closed without a copy of the order, but the court decision must be noted by the practitioner. If the order is received from the court within four weeks of the final hearing, it must be scanned and saved in ECMS.

9.10 Public and Private Law Cases:

9.11 Where a Service Manager has authorised a practitioner to close his/her case, the Service Manager is also responsible for periodically assessing the quality of the practitioner's closure practice, to be satisfied that the continuing delegation of closure authority is

justified. This assessment must be carried out at least annually and discussed/recorded in supervision, as set out in the Quality Improvement and Assurance Framework.

9.12 Where practitioners have been assessed as not meeting proportionate case closure or other service standards, or are within their first six months of employment with Cafcass, the Service Manager must review the file before closure, and electronically countersign the closure in the case plan.

9.13 Administrators must ensure that systems are in place so that cases can be closed promptly.

9.14 Administrators must ensure that such paper files as appropriately exist are boxed in accordance with the Cafcass storage and labelling protocol, with a note of the contents of each box filed electronically in a local Archive Register for easy retrieval. As ECMS is implemented, the Governance team is maintaining a centrally held spreadsheet of changes to location of closed paper files, for location changes post 14th July. Administrators must ensure that any changes to location of a closed case paper file (previously recorded on CMS) is provided to Governance as soon as the file is location is changed.

9.15 The closed case will remain in My Teams Closed Cases for one month, at which point it is automatically archived by ECMS.

10.0 Retention and deletion of ECMS and supplementary paper case information

10.1 Information arising from Cafcass' involvement in a case is to be retained until the youngest child who is the subject of the proceedings in the case has reached the age of 22 years. In cases where the child dies before the age of 22 years, the information is to be retained until the 22nd anniversary of the child's birth. At this point, the entire case record is to be deleted[7].

10.2 Within four weeks of the date of the final hearing, paper court bundles must be destroyed unless a decision is made that they need to be retained. Such a decision, and the reasons for it, must be recorded in ECMS.

10.3 In cases of exceptional sensitivity, including those where a future public interest issue may arise, the Head of Service and the National Service Director may jointly decide that the information must be retained for a longer period.

10.4 The Office Manager is responsible for monitoring the archive and ensuring that files are deleted once the retention period has expired.

11.0 Police information

11.1 Police information must always be retained for three months from the date of receipt, even if a WTFH case concludes earlier than that. This is because repeat checks may not be undertaken if a new application is received within three months of the date when a case is

[7] Detailed guidance of the deletion of all confidential information (not just case recording) is provided in the Information Assurance Policy.

closed, unless there is reason to believe that there has been police involvement in the meantime.

11.2 Information provided by the police, including international and military police, must be deleted 18 months after its receipt, or when the case is closed to Cafcass, whichever is the earlier. The exception is in WTFH cases, as in 11.1.

11.3 As set out in paragraph 4.7, the printing of third party information about service users is prohibited.

12.0 Continuity of business planning for case recording

12.1 In the unlikely event of ECMS failure, case documents must be stored temporarily on local G drives until such time as ECMS is restored. The Head of IT will issue a directive for the appropriate continuity process, depending on the type of failure being experienced.

Owned by	Anji Owens, Assistant Director
Approved by	OMT
Approved on	15 July 2015
Implemented	30th July 2015
Amended	• 4 September 2014: Paragraph 4.6 updated as agreed by OMT (August). • 20 November 2014: Appended guidance on how to share and transfer case related data (IAPB action). 30th July 2015: • Appended checklist on how to shield case information and added reference to this in the policy. • Note added at 2.1; that if two Guardians are appointed in the same case, there will be two separate case files on ECMS. • Clarified at 9.5 that there is no expectation to upload an order on a closed case unless this is an order for further work to be completed by Cafcass. • Clarified at 2.2 that it is the practitioner's responsibility to record diversity monitoring information on ECMS, in accordance with diversity monitoring guidance. • Added paragraph 4.8 • Updated appendix 3 following a management decision to use Royal Mail Services for our main secure postal requirements replacing DX.
Version	3.4 – replaced version 3.3 (January 2015).
Review date	August 2016

Appendix 1: Organisation of electronic case record

A spreadsheet setting out where each template should be saved is available on the ECMS page of the intranet.

Section	Title
	Case information This section should include the contact log report, the WTFH outcome form, and any detailed contact recording. Pre-14 July 2014 contact logs are saved as PDFs in the case information section. Detailed contact recording More detailed recordings should be stored separately from the contact log. The following is important: • Detailed recordings (such as the notes of interviews) can be stored separately from the contact log. A contemporaneous note has to be kept of meetings, including direct work with the child. • Handwritten notes can be scanned into ECMS if they are legible or, if they are not legible, they should be typed up. Once scanned or typed, the handwritten version can be destroyed. • Where handwritten notes are taken using OneNote or Word, using a tablet, they can be converted to text. The original handwritten copy (either in OneNote, Word, or converted to pdf) should not be saved in ECMS and can be deleted once the text transcription has been proofread by the author to ensure that it is an accurate copy of the handwritten note. • Notes should be saved under date of activity and type of contact. The use of the general term 'interview' should be avoided, unless it is also made clear whether it was conducted on a face-to-face basis or by telephone. • Detailed recordings should always include information about the date / time of the work; name of worker; name/role of every person involved; nature of contact; venue; brief outline of what happened; next steps agreed; and actions taken afterwards.
	The contact log The contact log is a running record of all actions in the case and should be cross referenced to other documents (detailed recording/case plans/Safeguarding letters/ position statements etc.). Pre-14 July 2014 contact logs are saved as PDFs in the case information section. From 14 July 2014 the contact log is built into ECMS and is both automatically and manually populated. A Word document can be generated with the content of the contact log, either to view as a document or to save as a PDF in response to a SAR. This document is not to be edited or updated or used as a running record or secondary contact log, and is to be deleted from the case record when no longer needed. If amending previous contact log entries, the reason for amendment is to be recorded. The modified date will be visible on ECMS and who modified the log, however the previous version will no longer be available. Manually entered contact log entries will include an automatic entry of the name of the staff member completing the entry and their role A suitable contact log heading should be selected, a summary of any information received and/or provided including the name/role of person spoken to or seen; and a note of any actions agreed should be included. In the record. If editing or amending previous contact log entries, the reason for amendment is to be recorded.

	Where items belonging to a service user are being stored on Cafcass premises, as part of arrangements for indirect contact, their location should be recorded on the contact log. Pre-allocation: The contact log can be started before allocation if any work is done by the service manager, business support staff, or duty practitioner (if applicable) if any work is done at that stage. In Private law, this commences on receipt of the C100 at the Cafcass Intake Team and should include the recording of screening requests, the requesting/receipt of screening information from LAs and Police, and the issuing of welcome letters. In WAFH and public law care cases, when a decision is made for the practitioner not to see a child as part of the work, the professional basis for this decision must be recorded in the case file.
	Correspondence Scan or save here all case-related correspondence, including the welcome letter and letter to parties, with the exception of: • Correspondence from any lawyer instructed by the Cafcass practitioner (saved in legal advice); and • Cafcass correspondence to the court if this is in place of a report (saved in reporting to court). Where case information is contained in emails, these must be saved into ECMS and must not be kept in Outlook. Emails must only be embedded into the contact log where they add to the case narrative and do not contain extraneous non case related information.
	Case Plan There is one case plan template in ECMS for use with both Private Law WAFH and Public Law cases. The guidance for using the case plan template is within the QA tool guidance – click here to access.
	Risk and safety process Scan and/or save here: • Information received in response to screening checks e.g. PNC record from the Police; to be deleted in accordance with Case Recording and Retention Policy; • Safety assessment documentation. For meetings you should still make a note on the contact log and cross-refer where appropriate to the detailed notes in this section; • any welfare referral; • notice to Children's Social Care of completion of case (where a referral has been made); and • Any tools used with parties. (Tools used with children are saved in Direct Work) Where no risk is identified from screening or during initial work, but is identified later, it must be recorded on the case plan and drawn to the attention of a manager either as part of formal supervision or ad hoc discussion.
	Reporting to court All templates are available in ECMS and should be accessed from ECMS Reports each time a new report is recorded. Scan or save here: • Reports, including Safeguarding Letter; and • Any correspondence to the court by the allocated practitioner, which is provided in

	place of a report, such as a letter to the court at the end of a Family Assistance Order for placing on the court file, advising of developments during the FAO.
	Direct work Scan or save here: all work done directly with the child or young person, including if the child met with the judge. Drawings, letters, and any other documents may require scanning to save in this section of the file. The use of any tools in direct work with children should be saved here.
	Court orders Scan or save all orders and directions made by the court. If these are contained within the separate court bundle, cross-refer in this section.
	Court papers Scan or save here: • Court papers including applications and statements; and • Any Cafcass information from a previous case. There is no requirement for court bundles to be scanned and stored in ECMS. Bundles can if necessary be kept securely in paper form for the life of the case and shredded at point of case closure.
	Experts & Agency Info Scan or save here: • Letters of instruction; • Notes of meetings with experts (if handwritten, must be legible); and • Experts' reports • Referral forms for contact services Other Agencies Other agency documentation such as copies of papers from the child's file; minutes of child protection conference.
	Legal advice This is privileged legal advice to Cafcass that is not to be disclosed. The purpose of storing this information in a separate section is to limit the risk of inadvertent disclosure, should a subject access request be received. Save or scan here: • Correspondence to and from Cafcass Legal; • Correspondence to and from the child's solicitor or other lawyer, who is instructed by the Cafcass practitioner; and • Notes of meetings and telephone calls with Cafcass legal, the child's solicitor or any other lawyer who is instructed by the Cafcass practitioner. Do not store here correspondence from the child's solicitor if there has been a formal separation between the young person and the children's guardian. In these circumstances, the correspondence will relate to the case but will not have the status of privileged legal advice.
	Further information Save or scan here any additional information, for example, any informal contact e.g. a thank-you card. QA tools should be stored outside of ECMS as they relate to the quality of work and performance of an individual. Decisions made during QA should be recorded in the case plan or contact log, whichever is more appropriate.

Appendix 2: Shielding case information check list

This checklist must be followed by FCAs (supported by Business Support Staff), when shielding case information on Cafcass case recording systems, in accordance with the Case Recording and Retention Policy.

Checklist	Action Completed?
How do I shield case information in CMS retrieval?	
➢ Run a person search on CMS retrieval, to find any associated cases in the legacy system. ➢ If there is case information in CMS retrieval, inform MIS about what CMS data needs to be shielded by sending the case number and the names of people to be shielded to the MIS National Office mailbox. ➢ **Please note:** All people related to a case should be shielded. ➢ MIS will manually shield the person/s and case record from CMS retrieval reports. ➢ The case will be marked as shielded and the only information that will appear on the report is the case number, the last allocated practitioner and the last allocated team. This information is to remain confidential within Cafcass, the existence of the case and all related information should not be disclosed to anyone external to Cafcass.	
How do I shield case information in ECMS Archive?	
➢ If a person search on CMS retrieval indicates that there is a related case/s, you need to then search ECMS archive for the case/s. ➢ If the case is on ECMS Archive, this needs to be shielded by dragging and dropping all documents from the ECMS archive folders to the shielded ECMS case. If an ECMS case does not exist please follow the below instructions to create one: 1. Create a new case on ECMS using the original application dates 2. On the Manage Case > Properties and Applications screen select the Case Factors drop down > Shielded Archive Case 3. Create a new manual contact log entry, select the Case Update heading to capture the original archived Case ID 4. Move all the documents from archive to the new case 5. Add a new contact log document to the archive that just has the Case ID number of the new case 6. Shield the new case (follow instructions below on how to shield a case)	
Is there any action I need to take before shielding case information on ECMS?	
➢ Managers and/or Business Support staff and/or Cafcass lawyers and/or Safeguarding Team will need to be co-allocated to a case, should they require access to the case when it is shielded for oversight or case administration.[8] ➢ The decision about who should have access to view a shielded case should be made by the Service Manager.	
How do I shield case information in ECMS?	
➢ On ECMS you shield the individual rather than the case. You therefore need to ensure that you shield every person associated with the case. ➢ To do this: Click into each *'person homepage record'* and on the far right click *'shield.'* Please note: This will automatically shield every associated case on ECMS with this person.	
How do I shield case information in G-drive?	
➢ Any associated casework on the G-drive must also be moved across to the shielded ECMS case folder (create a case folder using above instructions if there isn't one) and delete from G drive. ➢ Ensure you add a note to the ECMS contact log that this has been done.	
FCAs are also responsible for recording on the contact log:	
➢ the reason for shielding, ➢ the date of this action, and ➢ the persons who are to have access to the case. ➢ All actions taken to shield the case across all recording systems.	
Ask a colleague (who isn't allocated to the case on ECMS) to run a search on all systems to check that all case related information is shielded.	

[8] To allow a member of Business Support and/or a Cafcass Lawyer to be allocated (on ECMS) to a shielded case, this needs to be approved and requested by their manager by emailing the I-trent inbox and asking the person to be assigned an 'ECMS Champion' user role. You will then be able to co-allocate them to the case in ECMS.

Appendix 3: How to share and transfer case related data

Common information type	How information is generated	How information is received	Transfer reason	Transfer method
Other agency check requests (e.g. police/LA)	Internally	N/A	To request information from other agency for safeguarding check	Email via Egress*
Case information taken from files e.g. Subject Access Request (SAR) and complaints file	External case documents plus Cafcass generated casework	Cafcass holds this information.	SAR and Complaints file information requested by service users and possibly other organisations.	1) Email via Egress* 2) If no email address is available use Royal Mail Signed For
Case file	External case documents plus Cafcass generated casework	External information received by email and post	Case transfer between offices and handover to/from SEC.	Transfer between teams using ECMS. For hard copy files use Royal Mail Special Delivery Guaranteed or hand delivery
Service user correspondence including Welcome Pack, Safeguarding Letters and Court Reports	Both internally and externally		Correspondence with service user	1) Email via Egress*. Emails should only be sent to one email address to avoid disclosing email addresses to other parties (or use BCC). 2) If no email address is available: • Welcome Packs and appointment letters can be sent by standard Royal Mail but they must have a return address stamped on the envelope. • Safeguarding letters can be sent by standard Royal Mail with a return address; this is an accepted risk due to the need for quick turnaround. If there is concern over the sensitivity of the contents, these can be sent by secure/recorded methods. • Court reports and other post which gives a picture of the whole case should be sent by Royal Mail Signed For. 3) If the service user wishes, documents can be collected in person provided their identity is confirmed
Court correspondence	Both internally and externally	Email and post	Sharing information with courts	Email via Egress*

Solicitors/local authorities correspondence	Both internally and externally	Post/email/fax	Sharing information	Email via Egress*
HMCTS forms e.g. C100/C1A	Externally	Email from Courts/DX	Movement of case information between offices	Scan in document (National Business Centre/Warrington Digitisation Centre) and place on ECMS. Cases are transferred between teams via ECMS.
Other agency checks	Externally	Secure email	N/A: Checks should not be printed or shared in their original form.	

Notes & Glossary:

- * Egress encryption will :
  - send Egress secure emails to non-secure addresses: this includes .gov.uk.
  - send plain text emails to secure email addresses: these include addresses containing gsi, gcsx, cjsm, pnn or nhs.

- Cafcass staff are not authorised to send protected information to agencies and service users via non-secure email. Egress must be used for non-secure email addresses. 'Protected information' refers to safeguarding letters, court reports, case documents, and any other personal information relating to a service user.
  - Guidance on Egress for Cafcass staff can be found here on the Intranet.
  - Guidance for external recipients is here on the Cafcass website.

- Post options:
  - Royal Mail Signed For provides a secure postal method as it requires a signature of the recipient. 2nd class delivery is preferred as it has a higher successful delivery rate (99%), although if short timescales apply please use 1st class (93% successful delivery rate).
  - For particularly sensitive information, please use Royal Mail Special Delivery Guaranteed which provides a tracked service and consider double envelope.
  - For items over 2kg and under 20kg use Royal Mail Special Delivery; for larger items use an approved courier where necessary.
  - Please note DX is now only available in these offices:
- Bloomsbury (incoming and outgoing) subscription is to remain to assist the Legal Team
- Warrington (incoming only) is to remain enabling the courts to continue to send the standard documents currently received into Warrington to be digitised and uploaded onto ECMS.

- Cafcass staff are prohibited from printing personal/sensitive personal information provided by third parties (e.g. police, health bodies and local authorities) in all circumstances [see Section 4.7 Case Recording Policy].

- Cafcass case related documents containing personal/sensitive personal information (e.g. safeguarding letters and court reports) should not be printed or removed from Cafcass offices (including home-based offices) [see Section 4.6 Case Recording Policy].

GSI = Government Secure Intranet
GCSX = Government Connect Secure Extranet
CJSM = Criminal Justice System eMail
WTFH = Work to first hearing
DX = Document Exchange mail network
HMCTS = Her Majesty's Courts & Tribunals Service
SEC = Self Employed Contractor