Social Care Health and Wellbeing Directorate

SCS, OPPD, DCA, LD and MH, EYPS

Missing Care Files Policy and Guidance

Issue Date:	version 3a January 2017
Review Date:	January 2019
Owner:	SCS, Adults and EYPS Policy and Standards Team Operational Support Unit SCHWB Invicta House Maidstone Kent ME14 1XX

A copy of this policy is held on Tri-Ex and within EYPS, any changes MUST be reflected in all copies

POLICY

1. Principles

Principle 7 of the Data Protection Act requires that:

> Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This means you must have appropriate security to prevent the personal data being accidentally or deliberately compromised. In particular:

- design and organise security to fit the nature of the personal data held and the harm that may result from a security breach;
- be clear about who in your organisation is responsible for ensuring information security;
- make sure the right physical and technical security is in place and is backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

2. Scope

This policy and guidance applies to care files which have been accidentally lost, or destroyed, damaged or mis-placed within the EYPS and SCHWB Directorate. It relates to information about users of services only and does not include staff files and information.

The policy assumes steps are taken for the safe management of files in line with other record management policies.

<u>Kent and Medway Partnership Trust</u>

Where documents which hold information belonging jointly to KCC and KMPT go missing staff should follow procedure and reporting structures for both organisations. Where a missing file contains only KMPT information follow KMPT procedure.

3. Definitions

A “missing” care file is one that cannot be found or is not available when required for a service user encounter or other use by Council staff.

A care file is the electronic or/and hard copy file relating to a child or adult who uses KCC services.

Team Leader refers to the Manager with responsibility in a particular function, this may be Unit Leader, Team Manager or other title with the designated person being responsible for the day to day running of the client/ service user activity.

4. Context

The Data Protection Act 1998 requires that organisations which process personal data take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. KCC has put in place the Information Security Policy and The Information Security Incident Protocol.

5. National Guidance

Detailed information may be found on the ICO website:

5.1 Data Protection Principle 7
https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

5.2 Breach Management
An information breach can take many different forms, lost information, information sent to the wrong address and a range of other activities.
Information security breaches can cause real harm and distress to the individuals they affect – lives may even be put at risk. Not all security breaches have such grave consequences, of course. Many cause less serious embarrassment or inconvenience to the individuals concerned.
Information security breaches should be discussed with the Information resilience tand transparency team email: Informationgovernance@kent.gov.uk

http://knet/ourcouncil/Key-documents/Documents/Information%20security%20incident%20protocol.pdf
https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

or

5.3 ISO 270001 Standards:

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Practice Guidance

Where files have been lost or misplaced:

Search

1.1 Initial Search

a. If the file is shown as booked out and has not been returned, contact the individual concerned.

b. If not shown as booked out, carry out a physical check of the records storage area and check adjacent files in the same cabinet to rule out simple misfiling. If the file is tracked to another area, ask them to carry out a physical check of their area.

c. Check the overall summary of care activity on SWIFT/Liberi/EHM for any contact practitioners or other professionals. This may give clues as to who has handled the file. Speak to the individuals involved and ask them to carry out a search of their area.

d. Look at the previous history of file movement – speak to the individuals/ secretaries who have handled the file previously. Ask them to carry out a physical check of their areas.

e. If the Administration Officer is unable to locate the missing file this should be escalated to the Team Leader or their designated deputy who will complete a "Missing Care File – Search Log" (see Appendix A) and record this on SWIFT/Liberi/EHM.

f. When the Team Leader or a designated deputy has confirmed that the file is missing, a temporary file can be created and recorded in the "Temporary Care File – Log" (see Appendix B). This should be clearly marked as Temporary and a note made in the SWIFT/Liberi/EHM notes field.

1.2 Regular Searches

Periodically, the log should be consulted and summary checks made for the missing files listed. The dates searches are made should be recorded on the log sheet together with the name of the officer.

2. Missing File - Found

When a file is located the following procedure should be followed:

a. Update the missing care file log to show it has been located.

b. Merge the temporary or duplicate file with the original file.

c. Remove the temporary file indicator on SWIFT/Liberi/EHM.

3. Missing file - Lost

When a file has been missing for six months, it is reasonable to assume that the original file has been lost. Accordingly the temporary file should be converted into a duplicate file. The log of Missing Care File should be updated to reflect this change and a report made using the Information Security Incident Reporting Process.

4. Temporary Care Files

4.1 The temporary care file should be clearly marked as ‘temporary’ whether created as an electronic or hard copy.

4.2 The missing file should be recreated as far as possible, creating duplicate copies of any missing documents, these may be located in alternative settings. Duplicate copies must be clearly marked as duplicate, this will enable primary copies added at later dates to be amalgamated with the original file if found.

5. Missing (Open and Closed) Care Records – Reporting

5.1 KCC reporting

The Team Leader should complete a quarterly summary of missing care record files”. The number of missing and lost care records files must be reported to the Corporate Records Manager on a quarterly basis.

Where files are kept electronically, (for example in Liberi, Specialist Children Services case files), the team leader must follow the electronic missing case file guidance and procedures (link).

(see scope above for KMPT)

5.2 Informing the individual

5.2.1 Where a record has been deemed permanently missing a risk assessment is required to be carried out to consider the impact and possible consequences related to the lost file.

The risk assessment will consider:

i. The sensitivity of the information in the file
ii. The impact if the information is misused
iii. Was the information encrypted
iv. What happened to the information, lost in a KCC building, misfiled, removed from a KCC building and lost
v. How many files have been lost, multiple individual losses or a single loss of multiple files

vi. Who does the information relate to
vii. What are the risks associated with the information contained in the files, physical safety, reputation, financial loss, personal loss (e.g. adoption files)
viii. Are there wider consequences such as loss of confidence in KCC

5.2.2 The risk assessment should be completed for each missing file and consideration given to the impact on the individual whose records have been lost. A recommendation on whether to inform the individual should be discussed between the person with care responsibility and their manager. If necessary the line manager should seek advice from a senior manager.

In cases for the loss of individual files the Assistant Director or Head of Service, MH and Provision in social care or the Heads of Service in EYPS must approve the outcome of the recommendation.

In cases where multiple files have been lost the recommendations should be based on the information for each individual file, the recommendations will be collated by the Caldicott Officer and reported to the Caldicott Group. The Caldicott Group will ratify these decisions and escalate to the SIRO for final confirmation.

5.2.3 The guidance in the following table should be used to help in dealing with a request for information from an individual whose case is part of the accidental loss or destroyed multiple files.

	Low impact	Medium impact	High impact
Full reconstruction possible	Provide information	Provide information	Provide information
Partial reconstruction possible	Provide information with explanation for absences	Provide information with explanation for absences and offer further support	Invite to meeting
All information lost	Apologise	Apologise and offer further support	Invite to meeting

5.3 Informing the Information Commissioners Office

The Information Resilience & Transparency Team has responsibility on behalf of the SIRO for informing the ICO of any Information Security Incidents including lost records. The IR&T Team follow the ICO and KCC policy and guidance.

6. Monitoring

Each division should have arrangements for monitoring missing files and ensuring appropriate actions have been taken.

Monitoring should include:

- The line managers responsibility to identify and manage performance relating to practice and/ or repeated incidents.
- The Director responsibility to be informed about record management in their division and to be aware of the number of incidents and the risk management status.

Arrangements will differ due to the structures in each division.

Reporting should be at Divisional Management Team meetings and to the Caldicott Officer every 6 months.

Contacts

Caldicott Guardian:	Penny Southern
Caldicott Officers:	Janice Grant, Adults and Disabled Children Chris Nunn, Specialist Children's Services Katherine Atkinson, Education and Young People's Services
SIRO:	David Whittle
Data Protection Officer:	Ben Watts