Keeping Information Safe

Note: If printed, this document is for immediate reference only. Do not file it, as it will go out-of-date over time and be replaced by newer versions on-line. Always refer to the latest CMS version.

Security

All security, confidentiality and information sharing principles apply to electronic recording systems as well as paper systems. Mobile phones and personal digital assistants (PDAs) effectively act as mini-computers, and are subject to similar security threats and vulnerabilities, particularly when the internet, or email communication is involved.

Your employer is responsible for providing secure devices that are usable in real-life situations, and for agreeing and implementing effective and practical policies to cover the use and transfer of personal information, by whatever means. Electronic devices used for recording personal information are covered by stringent security requirements. Personal devices should not store any sensitive personal information but provide secure access to the council network; all mobile council devices should be encrypted; all emails containing sensitive personal information should be sent by a secure email network or encrypted using Egress.

Independent practitioners' security software and systems must meet business and personal information protection requirements. Computers and mobile phones may be used for both work and personal use but access to the council network must be via a secure way, for example, Egress.

Local standards

Do:

- Store all personal data securely, for example, in a locked cabinet and secure the key
- Securely dispose of all electronic personal data: for example, do not just delete items, ensure your desktop recycling bin is emptied regularly
- Delete information when it is no longer required
- Securely dispose of all paper based personal data using the confidential waste service
- Carry a locked briefcase or bag when transporting any data outside of the office
- Share data only when you are allowed to do so by law
- For sending and receiving sensitive personal information, use a secure email network, such as Egress Switch
- Send paper records containing restricted data using enhanced postal services for example, Royal Mail Recorded or Special Delivery

- Create your computer passwords using the password complexity rules, outlined in the Information Security Policy
- Report any data loss or theft including mobile devices such as USB sticks and laptops to your manager immediately
- Always 'lock' the desktop on your computer when leaving the desk
- Clear away personal data from your desk when you are not using it.
- Use Council issued memory sticks

Do Not:

- Create password protected documents
- Leave papers containing personal data lying on your desk unattended
- Store large quantities of personal data on the desktop or on the C drive of your computer
- Put any paper-based personal data in the normal waste or recycling boxes
- Store personal data on mobile devices such as laptops, smartphones or USB sticks without written approval from your line manager or the Caldicott Guardian
- Disclose your computer password to anyone or write it down on a piece of paper
- Send sensitive and protectively marked information outside the council using regular email
- Insert non relevant information into an email containing adult/carer information
- Leave notebooks/diaries unsupervised.

Physical Evidence

There is a secure drawer in zone 4B, store room 4.01. It is a drawer in the evidence room of the Fraud Team. It is for keeping evidence pertinent to social work matters such as safeguarding cases (DVDs, memory sticks).

Store in this drawer any evidence that cannot go on LAS that is physical evidence in a safeguarding Section 42 case. Log the evidence (in/out, date and by whom) in the book kept in the drawer.

Here are the golden rules of using the room:

- No worker ever accesses the room alone: a Safeguarding manager goes with the worker concerned to deposit or collect evidence
- Everything put in/ removed from the room is recorded in a book left in the drawer
- All evidence is labelled clearly (put it in an envelope and label the envelope)

The keys to the room are kept with the Safeguarding Team in zone 2C. Please ask a Safeguarding manager to accompany you once you collect the keys and return them immediately after using the room.

Lost Information

Practitioner: If information is lost, record in the person's Case Notes details of what information is lost. Report information losses to the Caldicott Guardian, currently the Head of Safeguarding and Quality Assurance. Be aware that lost information can incur fines on the department.

Take responsibility and exercise care when carrying information in both paper format and on devices, for example, a laptop, in public places. When it becomes known that some information has become lost, either through a system error, or when making a recording of a meeting outside your normal workplace, report that loss to the Information Management Team as a potential security/information protection incident and to the team manager at the point of discovery. Check the Council's process and requirements, and to report the loss, as applicable, to the individual concerned. Refer instances of lost information to the Croydon Council Information Management team and the Caldicott Guardian.