CHILDREN'S SERVICES AND ADULT SOCIAL CARE

PROCEDURE FOR THE SECURE STORAGE OF FILING CABINET KEYS

The purpose of this procedure is to set out the steps to be followed by employees working in social care related services with regards to the secure storage of filing cabinet keys where the filing cabinets are used for the storage of personal and personal sensitive information and equipment.

Principle 7 of the Data Protection Act states 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'. Adherence to this procedure forms part of our organisational duty of compliance with the Data Protection Act.

Where personal and personal sensitive information is stored manually (non-electronic format) employees must ensure the following is complied with:

- The manual records must be stored in lockable cabinets (this can include cupboards and other filing containers).
- Cabinets must be locked when not in use or when the office / room is left unattended.
- Copies of keys for all cabinets storing records must be kept in a secure location. This could include a key safe or digisafe, but if not available could be stored in a desk drawer or an office cupboard. Keys must not be left on desks or in open view.
- Keys must be kept within the office and not taken home or off the premises by employees.
- All employees with appropriate access permissions to the information stored within the cabinets must be made aware of the location of the keys.
- Managers should regularly monitor office security, checking storage areas for adherence to procedures and recording or reporting findings where necessary. Any issues should be reported to the Directorate Information Compliance Officer.
- No employee is permitted to have additional cabinet keys cut without prior consultation and permission from his/her line manager.

Services going through the Changing the Workplace Programme can request the provision of a key safe in their new accommodation. Those services not currently part of the Changing the Workplace Programme may choose to purchase a key safe or 'Digisafe'. If an office has a key safe, employees must ensure the following is complied with:

- All cabinet keys are returned to the key safe at the end of the working day and the key safe locked.
- If the key safe has a manual key locking system, the key for the key safe must be kept in a secure location. This could include a desk drawer or a locker for example. Keys must not be left on desks or in open view.

CHILDREN'S SERVICES AND ADULT SOCIAL CARE

PROCEDURE FOR THE SECURE STORAGE OF FILING CABINET KEYS

- All employees with appropriate access permissions to the information stored within the cabinets must be made aware of the location of the key safe key.
- If the key safe has an electronic or other code locking mechanism, the code for the key safe must be distributed to all those employees with appropriate access permissions to the information stored within the cabinets. The code must not be written down in hard copy i.e. on paper or notice boards.
- Key safe codes must be changed on a regular basis (no less frequently than every quarter) and when an employee leaves LCC or moves to a new job role within LCC. Key safe codes must be "strong" i.e. not 0000 or 1234.
- It is acceptable for key safe codes to be distributed to appropriate employees via email. Employees must not however, forward the code onto anyone who does not have appropriate access permissions.

Clear Desk and Screen Policy

Staff should adhere to the Clear Desk and Screen Policy.
http://insite.leeds.gov.uk/PoliciesAndProcedures/Documents/ClearDeskScreen.pdf

When files are left available on unattended desks, material could be removed from them and copied or stolen. To ensure that information is controlled and safe, employees should ensure files containing personal and personal sensitive information are removed from desks and returned to the designated secure storage when the employee responsible for the file:

- Has finished working on it;
- Is leaving his / her desk for a short while such as to attend a meeting or take a lunch break; or
- Is leaving the office for the day

Information security incidents

If an employee becomes aware of any information security related incident (which includes the loss or theft of paper records), or potential information security related incident, then the employee must immediately inform his or her line manager who will in turn inform the Directorate's Information Compliance Officer.

Similarly, employees should report any lost or stolen cabinet keys to his or her line manager.

Policy Statement

This procedure is underpinned by Leeds City Council's Information Security Policy and failure to adhere to this procedure may result in a failure to meet the standards outlined in the Information Security Policy.

CHILDREN'S SERVICES AND ADULT SOCIAL CARE

PROCEDURE FOR THE SECURE STORAGE OF FILING CABINET KEYS

Failure to meet the standards outlined in the Information Security Policy may be regarded as serious and any breach may render an employee liable to action under the Council's Disciplinary Procedure, which may include dismissal. The Disciplinary Procedure is part of the Local Conditions of Employment. Any disciplinary investigation resulting from a breach of this policy will be undertaken in accordance with the Council's Disciplinary Procedure.