Standard Operating Procedure: Guidance on handling personal information whilst out of the office

Author:	Matt Smith Head of Business Support
	Lewis Bourne Data Protection and Information Governance Manager

Date:	December 2019
Review Date:	December 2020

Purpose

This procedure is intended to:

- Support and contribute to our overall activities to keep all children and young people safe
- Provide all staff with detailed guidance on handling sensitive and special categories of information whilst out of the office
- Data Protection Law and the General Data Protection Regulation require staff to comply with a policy for processing Special Category and Criminal Conviction Personal data, this supports that policy that is available on Connect (IGPOL007).

Background

There are occasions when you will need to have special category (sensitive) information with you regarding a child, young person, family member or other individuals. Examples include: home visits; meeting; case conference.

This information is important to enable you to provide the level of support needed, make decisions, offer advice etc.

However, due care and consideration needs to be given at all times regarding the safety of the information and ensuring the information is not lost, stolen or accessed by unauthorised individuals.

General Data Protection Regulation (GDPR) and Data Protection Act 2018

Article 5, paragraph 1 (f) of the GDPR requires that personal data shall be:

Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Under the GDPR/DPA, personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category personal data is defined as any information relating to:

- Racial or Ethnic Origin
- Political Opinions
- Religious or other beliefs
- Trade Union membership
- Data concerning health, Physical or Mental Health
- Sex life
- Biometric or genetic information

In addition to the impact on safeguarding, loss of special category personal data is a breach of the GDPR and DPA and may lead to a monetary penalty to the council of up to 4% of annual turnover or £17 million (whichever is greater) and legal proceedings being taken against individual members of staff as well as disciplinary action.

Personal Responsibility & Accountability

Each member of staff has a personal responsibility to ensure information relating to children, young people and their families is kept safe and secure.

Negligent, reckless or deliberate mishandling of personal data in breach of Council policy, standards or guidelines and is considered possible gross misconduct.

Staff must notify their line managers immediately of loss or suspicion of loss of any confidential information or inappropriate disclosure. The GDPR requires serious data losses to be reported to the Information Commissioner within 72 hours of being discovered so prompt reporting is essential. Line managers are responsible for ensuring that appropriate action is taken to investigate and manage such incidents once the Corporate Information Governance Team (CIGT) have undertaken a severity assessment.

Managers must ensure staff are aware that disciplinary action may be taken when it is evident that a breach in confidentiality has occurred as a result of a member of staff's neglect in ensuring the safeguarding of confidential information.

Protocol / Procedure

The following section provides guidance on various issues when taking information out of the office.

Removal

Whenever you are contemplating removing information from the office to attend a meeting, home visit etc, it is first of all important to consider exactly what information is needed. Do you need the whole file, or will just certain parts be sufficient. The third GDPR Principle states:

Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation").

As a consequence, you could be in breach of GDPR by taking too much information out of the office.

If the information is in hard copy, would it be possible to take an electronic copy. This way the information will be stored on an encrypted device and if lost or stolen, will cause no impact on the family or any named individual.

If removing paper records, ensure a record is kept of any information taken out of and returned to the office. This way, at any time it will be clear who has what information and for what purpose. In the event of a breach, this can help in identifying exactly what information has been compromised and how the impact can be managed.

It is good practice to have a log book on the team and a record date; time, case reference or name and address, officer's name, purpose; counter signatory.

At all times, any information in your possession needs to be kept safe and secure and due care and attention needs to be afforded at all times to prevent any accidental loss or disclosure occurring.

Transport / Transit

When on route to your visit / meeting, you must ensure information is secure. Do not leave paper records, laptops etc on the seats of vehicles. Always store them in a secure place e.g. the boot of your car and keep it locked.

If taking information home in advance of a visit or meeting the following morning, never leave papers files or any device in the car overnight. Always keep the information or device secure in your house. It is also advisable not to keep the paper records with the electronic device. In the event of a burglary, a thief will target electronic devices and therefore by keeping paper records separate, will again reduce the impact.

Many data breaches have occurred when individuals leave confidential paper work in their laptop case. Please ensure old papers are removed from cases and destroyed securely, pay particular attention to this if sending your laptop back to Digital & ICT Services for repair.

Home Visits

Whenever conducting home visits or any scenario where other individuals are present, you need to ensure that only authorised individuals have access to the information. A few points to consider are:

- Do not leave any personal or sensitive personal material in the possession of anyone who is not authorised to view it. This includes parents, relatives and other organisation employees.
- Always check that someone is authorised to see material before disclosing it to them.
- Check, when handing papers over that they are only the papers that you want the person to have, that you have not picked the wrong material up from the printer or included someone else's records.

Destruction

All copies of original documents which have been taken out of the office must be destroyed in a safe and confidential manner on return to the office. Wherever possible, a cross cut shredder should be used, alternatively confidential waste bags must be used.

Anonymisation

Whilst conducting home visits etc, there will often be a need to make notes to enable you to complete your records fully when returning to the office.

It is good practice to ensure your notes, whilst they will still make sense to you are sufficiently anonymised to prevent anyone else identifying the individual. Ways to anonymise notes include only using initials, noting case reference numbers etc.

Advice and Support

All staff should ensure that they have completed their mandatory online training for Data Protection.

All Heads of Service are Information Asset Owners (IAO) for the information that their staff process, it is the IAO’s responsibility to ensure that this SOP is adhered to.

If you require any support or advice on any aspect of this SOP, please contact CIGT via email: information.governance@dudley.gov.uk or ext 5607.