**Storage of Data on Mobile Devices**

**Scope Of This Chapter**

This chapter provides guidance on the storage of personal data (including photographs) on mobile devices. 'Personal data' is any information about an identifiable living individual.

'Mobile devices' includes memory sticks, mobile telephones including smartphones, tablet technologies, netbooks and laptops.

**Relevant Guidance**

[**Guide to Data Protection (Information Commissioner's Office)**](https://ico.org.uk/for-organisations/guide-to-data-protection/)

See also [**Bradford MDC IT Policies and Procedures**](http://intranet.bradford.gov.uk/working-day) (Intranet access is required).

|  |
| --- |
| **Working from Home/Remote Working**  It is important to remember that principles of data protection and confidentiality apply equally when working in a home environment as they do when working in an office environment.  A home environment may pose additional risks and issues of which you must be aware.  See: [**Section 4, Working from Home/Remote Working**](https://bradfordchildcare.proceduresonline.com/p_storage_data_mob.html?zoom_highlight=Data+Protection#home). |

This chapter was added to the manual in January 2021.

1. **Introduction**

The Data Protection Act 2018 ('the Act') and the UK General Data Protection Regulations ('the UK GDPR') regulate the use of 'personal data' – obtaining, storing and processing it.

The purpose of the Act is to protect the rights and privacy of identifiable living individuals and to ensure that the data about them held, processed and used by organisations is managed properly. It places legal obligations on those who process personal information and ensures individuals are aware of and exercise some control over how information about them is to be used.

'Personal data' means any information relating to an identified or identifiable living individual.

'Processing' is defined very widely in the Act and will cover any activity carried out such as:

* Collection, recording, organisation, structuring or storage;
* Adaptation or alteration;
* Retrieval, consultation or use;
* Disclosure by transmission, dissemination or otherwise making available;
* Alignment or combination; or
* Restriction, erasure or destruction of data.

Advances in technology and increased use of mobile devices can present particular challenges and increased risk of data breaches, and all staff should be familiar with this policy.

The Information Commissioner's Office (responsible for ensuring compliance with the Data Protection Act) can and does impose substantial financial penalties for breaches of the Act.

**FAILURE TO ENSURE COMPLIANCE WITH DATA PROTECTION PRINCIPLES COULD LEAD TO DISCIPLINARY ACTION.**

1. **The Data Protection Principles**

The Data Protection Act has a set of principles on how to use personal data properly. Personal data shall:

* Be processed **fairly and lawfully**;
* Be processed for **specified, explicit and legitimate purposes**;
* Be **adequate, relevant and not excessive**;
* Be **accurate and kept up to date**;
* Be **kept no longer than is necessary**;
* Be **processed in a secure manner**.

1. **Use of Mobile Devices to Process Personal Data**

In order to ensure compliance with these Data Protection Principles in relation to storage of data on mobile devices, the following practice **must** be adhered to:

* Service-users must be informed of what data is to be collected and stored, and the reasons, including the extent to which the data will be used;
* All data must be securely stored;
* All data initially obtained on mobile devices must be held on such devices for the minimum period necessary, and should then be securely transferred to a secure network;
* The data must then be removed from the mobile device without delay.
  1. **Personal Data Shall be Processed Fairly and Lawfully**

Principle 1 in the Act states that 'personal data shall be processed fairly and lawfully'. In practice, this means that you must:

* Have legitimate grounds for collecting and using the personal data, and not use the data for any other purpose;
* Explain to the service-user what data you will be obtaining and how you intend to use the data;
* Handle peoples' personal data only in ways they would reasonably expect.
  1. **All Data Must be Processed in a Secure Manner**
* Personal data must only ever be stored on mobile devices provided for this purpose by the employer;
* Personal data must **NEVER** be stored on or transferred to staff members' personal devices such as mobile telephones, tablet or laptop computers, home computers, memory sticks, etc.
* Mobile devices should be password-protected and encrypted using encryption software which meets current standards to protect personal data - password protection alone is insufficient when the mobile device is handling personal data which if lost could cause damage or distress to individuals;
* Access to the device should be locked if an incorrect password is input too many times;
* The device should automatically lock if inactive for a period of time;
* Mobile devices should be equipped with software to enable the device to be tracked and remotely wiped of data in the event of loss/theft.
  1. **Staff Must Take All Practicable Steps to Maintain the Security of the Mobile Device**
* Only approved software (e.g. apps) must be downloaded onto mobile devices. Unapproved software/apps can compromise security of the device;
* Facilities such as wi-fi or Bluetooth, which could allow others to have remote access to the device, must be switched off – note that these are likely to be set to 'on' by default;
* Physical access to the device must be restricted – do not leave the device unattended or where it can be viewed by others. Keep the device with you or securely stored, e.g. in a locked drawer. **NEVER** allow others such as your own family members or the children of service-users to have access to the device.
  1. **Data Must be Kept No Longer Than is Necessary**

The Data Protection Act stipulates that personal data must not be kept for any longer than is necessary. All data initially obtained on mobile devices must be held on such devices for the minimum period necessary, and should then be securely transferred to a secure network.

* 1. **Secure Transfer of Data**
* A secure method must be used to transfer the data to a secure network as soon as possible – data should not be retained on the mobile device for any longer than necessary;
* Data can be securely transferred by secure email, direct transfer from mobile device to secure network computer or secure remote connection such as a Virtual Private Network (VPN);
* **NEVER** use personal email, unsecure email or cloud computing to send personal data;
* **DO NOT**use public facilities such as internet cafes to send personal data.
  1. **Photographs**

The Data Protection Act applies to photographs in the same way as to any other personal data, i.e. the collection and use of images (still or moving pictures) of any person who can be identified. The Act does not stop a person's image from being captured, but it does require the image to be obtained fairly, used for a legitimate purpose which does not cause the individual distress or prejudice and to be kept securely.

It is recognised that taking photos or videos of children/young people is a legitimate, and indeed an essential part of working with them, such as the recording of activities, at the request of the child or young person themselves, or for life story work. In all such situations staff should alert their line manager to the fact that photos or videos are being used and this should be recorded clearly in supervision notes.

Workers should also be sensitive to what photography might mean for a child/young person in that it may have been used abusively with some children/young people.

* The use of photography or reproduction of photographic images or the use of videos must always have a clear and child-centred purpose;
* Prior to the taking of any photo or video the purpose of this should be explained to the child or young person according to their age, development and understanding and to the parent/carer unless there are specific reasons not to do so in which case the child's/young person's social worker must give permission. A child or young person should not be photographed if they do not wish to be or if their parent/carer/worker does not wish them to be;
* In relation to one-to-one work by staff with children, written consent should be gained from the child's social worker or parent/carer and placed on the child's file unless the young person is clearly of an age and understanding to give informed consent on their own behalf. Key workers must then check that consent is on the child's file before taking images. For the purpose of group activities when photography is frequently used, carers/social workers should be notified and written consent gained;
* Children/young people must be clothed and their torsos covered when being photographed or videoed. Cultural and religious traditions of clothing must be observed where needed;
* Staff must not take any photographic images of children/young people to their own home or keep them in their private possession;
* If photos or videos are to be used for public display e.g. for publicity purposes, specific permission must be sought from anyone with **Parental Responsibility**, parents/carers/social workers and from the child/young person if appropriate. A separate consent form will be used for this particular purpose and children must always be dressed in the images. The name of the child/young person in the image must never be used;
* Images of children must not be posted on facebook or any other social networking internet pages.
  1. **Reporting Security Incidents**

Staff should immediately notify their Manager of any loss, theft or wrongful disclosure of personal or sensitive data/mobile devices.

1. **Working from Home/Remote Working**

It is important to remember that principles of data protection and confidentiality apply equally when working in a home environment as they do when working in an office environment.

A home environment may pose additional risks and issues of which you must be aware.

For instance:

* Ensure that confidential material and devices containing such material (eg phones/laptops) cannot be viewed or accessed by other members of the household. It is important to make sure that children and pets, for instance, do not have access to work laptops. It must be remembered that the same rules apply to adult members of your household, such as partners;
* If you have paper copies of personal data, these must be disposed of securely, i.e. by shredding;
* Be mindful of ensuring that confidential telephone conversations cannot be overheard;
* Beware of 'smart home' devices (Alexa, Google Home, Nest, Ring, 'nanny cams' etc.). These devices may be 'listening' in to conversations and/or 'watching'. These devices must be disabled if they are sited close to where you are working;
* Cloud storage should not be regarded as secure unless specifically provided and approved by your employer. Likewise with personal devices such as telephones and computers;
* Remember that you are still working, and appropriate standards of professionalism should be maintained at all times.  Do not post anything on personal social media accounts that could inadvertently disclose any confidential work material/issues/identifying information in relation to service-users.