



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

Data in transit policy

Statement

This document is intended to prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security when using, taking or sending sensitive or confidential data outside of their normally secure location. The need for this is driven by our duty to protect the information of individuals and Hartfield Playschool.

Other relevant Policies and Guidance: The policy does not stand alone, but should be read and acted upon in conjunction with the following Policies: - Data Protection Policy and E-Safety Policies.

This duty arises from legislation relating to information security, the most notable of which is as follows:

- Data Protection Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 2000
- GDPR May 2018

Sensitive and confidential data must be treated with appropriate security by all who handle it. 'Appropriate' is not defined in terms of hard and fast rules, but is meant to be a degree of precaution and security proportionate to the potential impact of accidental disclosure. It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data **MUST** assume personal responsibility and make considered judgements in terms of how they handle data whilst maintaining their role and responsibilities and if any doubt seek support from the Business or Early Years Manager.

Consider: If you were working on very sensitive and private information about yourself, carrying it with you or sending it to someone what would you do to protect it?



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

3. WHO THIS POLICY APPLIES TO

This Policy applies to all circumstances where sensitive or confidential data is taken outside of its normally secure location. This includes data in all formats: non-electronic (paper) and electronic (e.g. on PCs, tablets, laptops and removable storage media, e.g. USB memory sticks, etc.)

Whilst the Policy refers to employees, it also applies to all contractors, temporary staff, volunteers, trustees, work experience candidates, and all other agencies that use our data.

4. RESPONSIBILITIES

Hartfield Playschool maintains appropriate security and privacy of data that it uses to perform its functions and it will ensure that appropriate tools, training and guidance are available to staff.

- Secure network and pin protected
- Secure work locations for storing and using hard-copy data eg Office PCs

5. PLAYSCHOOL PROCEDURE

In the event that a member of staff needs to take equipment out of the building eg laptop, memory stick, tablets or paperwork which contain information about staff, families or children then they must obtain the permission of the Early Years manager or Business manager. All staff have permission to take their tablets home but all should only log on within their secure network at home

6. 'COMMON SENSE' PRECAUTIONS

There are some 'common sense' precautions that you can take before sending or taking sensitive or confidential data outside of its normal secure location.

These are:



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

- Check that you are not sending/taking more detail than is necessary i.e. will the information still meet the need if you remove the sensitive material.
- Check that the data you are sending/taking is correct and appropriate
- Check that you are sending the data to the correct person/address
- Check how you intend to keep it secure

As set out above, the precaution and security should be proportionate to the potential impact of accidental disclosure. It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data **MUST** assume personal responsibility and make considered judgements in terms of how they handle data whilst maintaining their role and responsibilities and if any doubt seek support from the Business or Early Years Manager.

Overall impact is determined by the degree of sensitivity of the data and the quantity involved, but we must remember that a single record about an individual can have a potentially massive impact on that individual if accidentally disclosed to others.

7. METHODS OF SENDING DATA

The following is a list of methods and devices commonly used to store and/or transfer data outside of their normally secure location. Email, Post, Home PC/Laptop

- **Mobile Devices:**
 - o Laptops and Tablets
 - o CD/DVDs
 - o USB Flash/hard drives –memory stick

However, listed below are methods which are ranked in categories of security and preference and it is your responsibility to ensure that you use a method and degree of security appropriate to the sensitivity, quantity and potential impact of the data being handled.



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

APPROVED SECURE TRANSFER METHOD

These are secure transfer mechanisms already in use and approved as secure for the purpose.

Examples of this are:

- Make sure the recipient is known and trustworthy
- Make sure it is traceable (apply delivery and read receipts) where possible

Web Portal

If you are transferring sensitive or confidential data through a web portal you must:

- Ensure that there is robust access control in place (i.e. unique user name/password)
- Ensure that only the people who need the data can see it
- Ensure that the data has https connection

Mobile Storage Devices

If you are taking data with you on a mobile storage device, such as a tablet, laptop or a USB memory stick and you must:

- Make sure that there is no other more secure option available to you
- Only use Hartfield Playschool approved storage devices
- Take only as much as necessary, for as long as necessary and transfer it back to its normally secure location as soon as possible
- Keep passwords separately from the device/data
- Take all reasonable precautions to keep the device and data safe and secure e.g.
- Keep it with you whenever possible, lock it away securely when you can't



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

- Never take it out in public places
- Never let others use your access or device
- Delete the data from the device as soon as possible
- Report loss/theft immediately

Post

The postal service is considered reasonably secure for small amounts of low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data).

There are precautions that you must take to prevent loss:

- Make sure that the recipient and destination address is correct, accurate and up-to-date
- Clearly mark the envelope/parcel with a return address in case of incorrect delivery
- Do not send the only copy of the data if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- If you use a courier they must be known and trusted
- Make sure it is traceable (i.e. confirmation of receipt or recorded delivery)
- Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

7.6 Home PC/Laptop

If you are working at home on your own PC or laptop you must:

- Only work on sensitive or confidential data that you can access. You must not transfer sensitive or confidential data to your home PC or laptop from any other source



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

- Only have as much sensitive or confidential information open as necessary and only for as long as necessary – do not save the data on your machine and do not leave the connection open when you are not actively working on it
- Always save the data back to their normally secure location when you have finished
- You must not leave the computer unattended for any period of time such that others can access any sensitive data; always log out when you are not using it

7.7 Physical (Paper) Records

If you are taking sensitive or confidential information with you in non-electronic (paper) records you must:

- Make sure that there is no other option available to you
- Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable
- Take only as much as necessary and only for as long as necessary
- Transfer it back to its normally secure location as soon as possible
- Take all reasonable precautions to keep the records safe and secure e.g.
 - ✓ Keep it with you whenever possible; lock them away securely when you can't
 - ✓ Use a suitable container that prevents accidental loss and/or viewing by others
 - ✓ Never leave it in plain sight in public places
 - ✓ Report loss/theft immediately

DATA HANDLING METHODS TO AVOID



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

There are some data handling methods which simply must be avoided:

- Sending sensitive or confidential information in unencrypted electronic form at any time without taking appropriate precautions as set out in this policy and guidance.
- Storing sensitive or confidential data on any personal equipment
- Sending sensitive or confidential information as unsecured physical records.
- Working on sensitive or confidential data on a public PC/laptop (for example in a library or café).
- Working on sensitive or confidential data on a PC or laptop with an unencrypted wireless (WiFi) connection, i.e. ensure your home wireless network has encryption and use it.
- Leaving sensitive or confidential physical records in plain view of others (i.e. on the back seat of your car, in a public place, on your kitchen table or even with you, but where they can be overlooked by others).
- Leaving any device holding sensitive or confidential information unattended in plain view of others.

REPORTING DATA LOSS In the first instance staff should report a loss of sensitive and/or confidential data to the Early Years manager and Business Manager.

DEFINITIONS

Sensitive and Confidential Data

The following list is not exhaustive and contains examples of sensitive and confidential data:



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

- a) Any data covered by the Data Protection Act – i.e. all data that relates to a living individual
- b) Any data that relates to commercial proposals or current negotiations.
- c) Any data relating to security information, investigations and proceedings, information provided in confidence etc.

An easy sense check on whether data is sensitive or confidential is:

- Whether the data is covered by the Data Protection Act 2018
- Could release of the information cause problems or damage to individuals, the public or Hartfield Playschool (*This could be personal, financial, reputational or legal damage*)
- Could release prejudice the outcome of negotiations or investigations? If in doubt ask your manager and err on the side of caution – treat it as sensitive and confidential – do not assume that it is not.

Normally Secure Location

For the purposes of this policy standard ‘normally secure location’ is defined as:

• A secure network/storage facility with:

- ✓ Access controls such as individual login accounts
- ✓ Backup and recovery facilities
- ✓ No public access
- ✓ Anti-virus and firewall protection
- ✓ Secure buildings or parts of buildings with: *Physical access controls – key pads, keys etc.*
- ✓ No public access
- ✓ Lockable storage facilities
- ✓ Other protection systems e.g.: alarms, security lights etc.



Statutory framework requirement: Information and records

Providers must maintain records and obtain and share information. Records relating to individual children must be retained for a reasonable period of time after they have left.

Encryption

Encryption is the process of transforming information to make it unreadable by anyone who does not have an appropriate 'key' or password. Those who have an appropriate key or password can use it to reverse the encryption process (known as decryption) to enable them to read the information.

This policy was reviewed by the Early Years Manager: Debbie Arnett and adopted by Hartfield Playschool staff and trustees in October 2022.

Name of Early Years Manager: Debbie Arnett

Signature:

Name of Registered Person and trustee: Sarah Adams

Signature:

Signed and agreed by all staff

Charlie Heath

Terri Ward

Katie Woodley

Alex Chapman

