



Data Protection Policy

Glossary of Terms used in Data Protection documentation

Data	Any information relating to a data subject, e.g. name, address, date of birth, etc.
Data Subject	The person to whom the information relates, e.g. Child, parent, staff, and committee members.
Data Controller	The Early Years Group, as a separate entity, is the Data Controller. However, responsibility for data protection matters is usually delegated to an individual, e.g. Chair of the management committee and/or the early year's group leader. The Data Controller acting in accordance with the six Data Protection Principles as outlined in the Data Protection Act 2018 decides how the required information will be obtained, processed, stored, updated, disclosed, disposed of/destroyed (see Appendix 1).
Data Processor	Processes data on the instructions of the Data Controller.

Data Protection Policy Part I

Purpose and Remit of Policy

To work effectively The Old Station needs to gather and process relevant information (data) about the staff, parents, children and professionals and others (data subjects) involved in the day-to-day running of the group. This will be done in accordance with the principles specified in Part II of this document. A designated person (data controller) will decide what information is required and how it is to be obtained. This information will be handled by a person(s) (data processor) acting on the instructions of the data controller and in accordance with Part II of this policy.

The Old Station by adhering to this policy (Part I and Part II) will ensure that data is handled properly and confidentially always and in accordance with the Data Protection Act 2018. This applies to data held on paper and by electronic means.

The Old Station recognises its responsibility to ensure that all persons acting on behalf of the group are made aware of this policy and receive any necessary training.

Part II of this policy covers:

- data collection;
- data storage/security;
- data updates;
- data disclosure;
- data access;
- data disposal/destruction.
- use of CCTV
- rights of data subjects
- complaints

The Old Station will review this policy annually to ensure that:

- data is collected fairly, used lawfully and in a transparent way
- data is collected only for valid purposes
- data is adequate, relevant, and not excessive;
- data is accurate and up-to-date;
- data is stored securely;
- data is only retained as long as is necessary;
- new staff/parents are made aware of the policy.

Data Protection Policy Part II

1.0 The Old Station will comply with:

- 1.0 The terms of the 2018 Data Protection Act and the General Data Protection Regulation (EU)2016 and any subsequent relevant legislation (Appendix 1).
- 1.1 Any guidance on or update to this policy notified by NIPPA – the Early Years Organisation.

2.0 Data Collection

- 2.1 Only relevant personal data will be collected by both electronic and manual means. The data collected in relation to staff during employment is for the purposes of the Nursery's administration and management of its employees and business and for compliance with applicable procedures, laws and regulations. Electronic recording may include computers, CCTV systems, digital cameras, smartphones, credit card machines, call logging and recording systems, clocking machines and audio-visual capture, My Nursery Pal and storage systems.
- 2.1 The person(s) from whom it will be collected will be informed of its uses and of any possible disclosures that may be made.
- 2.2 Systems will be put in place to facilitate updating information held (Appendices 4, 5).

3 Data Storage/Security

- 3.1 Manual data will be stored in a secure place only accessible to those with a legitimate reason to view/use that data.
- 3.2 Electronic data (if applicable) will be protected by password. If the computer is connected to the internet, a firewall system will be used.
- 3.3 Computer (if applicable) will be positioned to ensure that information is not visible to a casual observer.
- 3.4 Sensitive personal data, e.g. medical records/child protection records/interview material will be stored using a coding system and access will be strictly limited (need to know basis) and recorded.
- 3.5 Computers holding personal information are password protected, staff do not share passwords and individuals have their own log-in facility. Users 'log out' when the computer is left unattended.
- 3.6 Up to date virus protection software is installed on all administration computers.
- 3.7 Permission is sought from parents during the registration process for us to communicate electronically. Email addresses will be stored in group contacts
- 3.8 Managers and leaders are only permitted to store personal information on USB memory sticks which stay on the premises
- 3.9 Confidential paper based information such as addresses and telephone numbers are kept in the nursery office which is locked at the close of business each day
- 3.10 Room registers will be stored in a locked cupboard/ filing cabinet overnight
- 3.11 When using internal/external postal systems; information and documents are to be dispatched using sealed envelopes
- 3.12 The nursery disposes of confidential or sensitive documents via a shredding system.

3.13 All staff and students receive a copy of the nursery confidentiality policy and sign a confidentiality agreement slip.

4 Data Update

4.1 Forms will be issued to staff/parents/others to ensure that data held is up-to-date and accurate (Appendices 4, 5).

4.2 It is your responsibility to ensure that data we hold about you is up-to-date.

4.3 Data held will be updated promptly on receipt of appropriate form. If incorrect/out of date data has been disclosed to a third party, recipient will be informed of corrected data and this will be recorded.

5 Data Disclosure

5.1 The consent of the data subject will be obtained before the group discloses personal information to any organisation or individual.

5.2 All requests for disclosure will be in writing and telephone enquirers advised accordingly.

5.3 In cases of child protection, the law requires the disclosure of information, without consent, to relevant Social Services personnel and P.S.N.I. officers.

5.4 If a request for information relating to child protection is received by telephone, steps should be taken to ensure that such information is disclosed to identifiable personnel (i.e. seek verification of identity) and only if the individual is entitled to receive that information (authorisation). It is advisable to disclose such information only to those known to be involved in child protection. If doubt exists, ask enquirer to route enquiry through a known channel. Always call an enquirer back and be very alert if the number given is that of a mobile telephone.

5.5 Requests from parents for a printed list of children's names/addresses will be politely refused.

5.6 Personal data (including images) will not be used in newsletters, websites or in other media without the consent of the data subject (see Appendix 6).

5.7 The conditions outlined in Appendix 6 will be adhered to strictly.

5.8 A record will be kept of any data disclosed so that recipient can be informed should data be updated / altered at a later date.

6 Data Access

6.1 Data subjects have the right to access any personal data held about them.

6.2 Any person(s) wishing to exercise this right must make a request in writing to the Data Controller. It will assist in providing the requested data if forms (Appendix 2 or 3) are used.

6.3 You may, within a period of one month of your written request, inspect and/or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections should such records be faulty. If you wish to do so you must make a written request to your immediate Manager.

6.4 The information will be made available as soon as possible and within one month period recommended by the Data Protection Act 2018.

6.5 Any delay occasioned by the necessity to consult with an appropriate healthcare professional in relation to a data subject's medical information will be explained in writing to the individual making the request.

7 Data Disposal/Destruction

7.1 The Data Controller(s) will review personal data regularly and delete information which is no longer required for the purposes of the group.

7.2 The Data Controller(s) will keep a deletion file and record the type of deletion and the date on which it occurred.

7.3 The Data Controller(s) will not delete information relating to accidents on the premises or child protection issues until the required statutory period has expired.

8.0 Removal of information from the premises

From time to time Managers, Supervisors and Nursery Practitioners may take documentation away from the premises to complete work at home. In these instances prior permission is needed from the Management. See also Personal Data Breaches (below).

The following steps are in place to minimise the risk of loss/ damage/ impropriety;

- 8.1 All documentation removed from the premises is returned within 24 hours, or 48 hours over a weekend period.
- 8.2 Temporary storage of documents away from the place of work must be inaccessible to family/ residents or visitors
- 8.3 Confidential documentation no longer required must be returned to the nursery and disposed of as outlined in the section 'information security'
- 8.4 Documentation and lap tops should be transported in the boot of the car out of sight
- 8.5 Documentation and lap tops are not to be left in vehicles overnight.

9.0 Notification to the Information Commissioner's Office

- 9.1 The Information Commissioner maintains a public register of data controllers and The Old Station Nursery is entered on this register. The Data Protection Act 2018 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The registered data controller for The Old Station Nursery is:

Carolyn McDonald-Proprietor/Manager

and is the person responsible for notifying and updating the Information Commissioner's Office.

The register entry for The Old Station Nursery contains personal data held for 6 purposes.

1. Staff Administration
2. Advertising, Marketing and Public Relations
3. Accounts & Records
4. Provision of Child Care
5. Education
6. Crime Prevention & Prosecution of Offenders

10.0 Special Provisions - CCTV

The Old Station Nursery is dedicated to providing the highest standards in care and education for nursery and pre-school children. A Closed Circuit Television (CCTV) system provides a way of improving the safeguarding of children and staff who attend the setting.

The CCTV system is owned solely by The Old Station Nursery and has been installed to fulfil the following objectives:

1. To protect the assets of The Old Station Nursery
2. To increase personal safety and reduce the fear of crime, in particular, access to the building by people whose intent is to cause harm to children or staff of The Old Station Nursery.
3. To support the police in a bid to deter and detect crime
4. To assist in identifying, apprehending and prosecuting offenders
5. To protect members of the public and private property & staff

10.1 Practice

The CCTV system is registered with the Information Commissioners Office and follows the requirements of the Data Protection Act 2018 (the Act). The Old Station Nursery will seek to comply with the requirements both of the Data Protection Act and the Commissioners Code of Practice. The Old Station Nursery will treat the CCTV system and all images, information, documents and recordings obtained and used as data which are protected by the Act in the strictest confidence.

CCTV Cameras will be used to monitor activities within the Main Hall, Stairway to second floor of the main building, Baby/Wobbler rooms, Toddler room, Pre-School room, Playgroup/Afterschool Club rooms, kitchen in the mobile building, nursery office and outdoor play areas. For reasons of crime prevention and unlawful access to the building outside of The Old Station Nursery hours, the system is in continuous operation.

Children's changing areas and all toilets in the building are deemed inappropriate for monitoring purposes. These areas are not covered by the CCTV Cameras.

Private dwellings and property are not covered by the CCTV cameras.

Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained, as set out in the Regulation of Investigatory Power Act 2000.

Images will only be released to the police for use for the investigation of a specific crime and with the written authority of the police.

Images will not be released to the media unless this has been agreed by parents/Carers or other individuals who are pictured in the images.

No images will be released to anyone for the purposes of entertainment.

The planning and placement of CCTV cameras has sought to ensure that the system will give maximum effectiveness and efficiency for its registered purposes, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Signage stating the use of CCTV, as required by the Code of Practice of the Information Commissioner has been placed at all access routes to areas covered by the CCTV system and additionally directly beneath each camera.

10.2 Operation of the system

The scheme will be managed by nursery managers, in accordance with the principles and objectives expressed in this policy.

The control panel will only be operated by manager of The Old Station Nursery.

The CCTV system will be in operation 24 hours a day, every day of the year.

10.3 Control of Cameras

The Manager/s will, on a daily basis check that all cameras are functional from a monitor situated in The Old Station Nursery office.

Unless an immediate response to events is required, staff will not direct cameras at an individual or a group of individuals. Authorisation to redirect any camera must be obtained from the Manager, as the registered controller of the system.

Administrative functions will include the maintenance of hard disc space.

10.4 Monitoring Procedure

Camera surveillance may be maintained at all times.

A monitor is installed in The Old Station Nursery office where management staff can monitor the activities of the Nursery, limited to the rooms stated previously. The Nursery office is kept locked at all times when the Nursery is not open for business.

The system has the facility to store images to the hard drive and also to external devices if required. These external devices are CD/DVD/ or memory devices requiring a physical connection to a USB port. The transfer of images to these devices will only be carried out with the authorisation of Carolyn McDonald Proprietor/Manager. Such occurrences of any transfer of images will require a record being entered in the CCTV log book that includes:

1. Each record made must be uniquely identified, using a naming convention that follows a format of room, date, time of the image record being taken.
2. Before using each recording, any previous recording made on the media must be erased.
3. The controller shall register the date and time of when the image record was transferred, including the unique mark reference.
4. A recording required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure store. If the record is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to secure storage.

10.5 Access to records

By legal authorities

Recording media may be viewed by designated operators and the police for the prevention and detection of crime.

A record will be maintained of the release of records to the police or other authorised applicants.

Viewing of records by the Police must be recorded in writing in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 2018.

Should a record be required as evidence, a copy may be released to the police under the procedures described in this policy. Records will only be released to the police on the clear understanding that the record remains the property of The Old Station Nursery, and both the record and information contained on it are to be treated in accordance with this code. The Old Station Nursery retains the right to refuse permission for the police to pass on the record or any part of the information contained therein to any other person.

The Police may require The Old Station Nursery to retain the stored records for possible use as evidence in the future. Such records will be properly indexed and securely stored until they are needed by the police.

Applications received from other external bodies (e.g. solicitors) to view or release records will be referred to Carolyn McDonald Proprietor/Manager.

A charge of £10 will be made to cover the costs of producing the material. This charge applies to any authorised person requiring a copy of recorded images from the CCTV system.

10.6 Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to view data held about themselves, including those obtained by CCTV.

Requests for Data Subject Access should be made in writing to Carolyn McDonald. In most cases a valid subject access request will receive a response within one month of receiving the request. If an individual requires a copy of any images recorded on the CCTV system, then this will be subject to a charge to cover the cost of producing the material, as previously outlined.

Digital recordings will be kept for a maximum of 28 days, unless specific incidents have been recorded subject to further investigation.

Breaches of the policy and code (including breaches in security)

Any breach of this policy by The Old Station Nursery staff will be initially investigated by Carolyn McDonald Proprietor/Manager in order for her to take appropriate disciplinary action.

Any serious breach of the Code of Practice will be immediately investigated and recommendations made on how to prevent any repetition of the breach.

Complaints

Parents concerned about any aspect of the management of personal data within the nursery are able to raise their concerns in a fair and equal way. Complaints can be registered with the Nursery Manager. If individuals remain unsatisfied that their complaint has not been properly dealt with then they should report this to social services.

Appendix 1

Data Protection Act, 2018

To comply with the law all early years groups collecting and storing information relating to individuals must comply with the Six Data Protection Principles which are set out in the Data Protection Act of 2018.

These principles require that personal data shall:

1. Be obtained and processed fairly and lawfully in a transparent way.
2. Be obtained for a specific and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. Be adequate, relevant, and lawful and not excessive for those purposes.
4. Be accurate and kept up to date.
5. Not be kept for longer than is necessary for that purpose.
6. Be kept secure from unauthorised access, accidental loss, or destruction.

See also The Old Station Day Care Nursery's Privacy Notice for Staff, and Parents / Guardians / Children

Your Rights:

Under Data Protection legislation you have several important rights free of charge. In summary, those include rights to:

- access to your personal information, by means of a subject access request
- require us to correct any mistakes in your information which we hold
- require the deletion of personal data where there is no good reason for us to continue processing it
- object at any time to processing of personal data concerning you for direct marketing
- object in certain other situations to our continued processing of your personal data
- request that we restrict our processing of your personal information e.g. to confirm accuracy or the reason for processing.
- Request the transfer of your personal data to another party.

For further information on each of those rights, including the circumstances in which they apply, contact the UK Information Commissioner's Office (ICO) at <https://ico.org.uk>

If you wish to exercise these rights, please contact your Manager in the first instance. No fee is usually required. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact your Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Personal Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by staff;
- sending personal data to an incorrect recipient;
- electronic devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

If an employee suspects a breach whether actual or not, it must be reported immediately to the Manager to be registered and investigated. This will facilitate decision-making to ascertain if The Old Station Nursery is required to notify the relevant supervisory authority and the affected individuals.

All breaches will be investigated to assess whether the breach was a result of human or systematic error and put measures in place to prevent such a breach in future.

This policy will be reviewed annually by the management team to ensure it remains fit for purpose.

Signed: _____
(On behalf of the management team)

Position: _____

Date: _____

Reviewed on:

Date: _____ Signed: _____

Date : _____ Signed: _____