



UK GDPR/Confidentiality Policy

Manor House Minster Nursery are committed to protecting your privacy and keeping your personal data secure. We will only use your (including your child's) personal information to provide a service to you. We will keep your information secure and will never share it except if required to do so by law.

What is Personal Data?

Personal Data is data that can be linked to a single person which identifies them in some way.

Manor House Minster Nursery hold the following information for

Parents/Carers and children;

- Name of parents/carers
- Personal email address (a generic email e.g. info@ is not a personal data unless it can be linked to more data stored elsewhere)
- Name of the child
- Postal address
- Telephone numbers
- Marital status
- Date of birth
- Attendance information
- Characteristics including ethnicity, language, pupil premium etc.
- Development summary/reports
- Special educational needs information
- Medical details

UK GDPR is a regulation covering data protection and stands for General Data Protection Regulation.

We collect and use personal information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6(1)(e) and Article 9(2)(b) of the UK General Data Protection Regulation (UK GDPR). We will ensure that staff understand the need to protect the privacy of the children in their

care as well as the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality.

At Manor House Minster Nursery we have an open access policy in relation to accessing information about the nursery and parents' own children. This policy is subject to the laws relating to data protection and document retention.

Parents are welcome to view the policies and procedures of the nursery which govern the way in which the nursery operates. These may be viewed at any time when the nursery is open, simply by asking the duty manager. The nursery managers or any other relevant staff member will also explain any policies and procedures to parents or use any other methods to make sure that parents understand these in line with the nursery's communication policy.

Parents are also welcome to see and encouraged to contribute to all the records that are kept on their child. However, we must adhere to data protection laws and, where relevant, any guidance from the relevant agencies for child protection.

Legal Requirements

- We follow the legal requirements set out in the Statutory Framework for the Early Years Foundation Stage (EYFS) and accompanying regulations about the information we must hold about registered children and their families and the staff working at the nursery.
- We follow the requirements of the Data Protection Act (DPA) 1998 and the Freedom of Information Act. We keep two types of records on children attending our setting:
 1. Developmental records
 - These include observations of children in the setting, samples of their work, summary developmental reports and records of achievement.
 - These records are written and stored on the FAMILY app and can be accessed, and contributed to, by staff, the child and the child's parents.
 - Safeguarding files and Children's individual development support plans for SEND
 2. Personal Records
 - These include registration and admission forms, signed consents, and correspondence concerning the child or family through the Impact Early years data base, reports or minutes from meetings concerning the child from other agencies, an on-going record of relevant contact with parents, and observations by staff on any confidential matter involving the child, such as developmental concerns or child protection matters.

Parents/Carers consent to Manor House Minster Nursery storing their personal data and sharing if legally required to do so when signing the child's registration form which also requests specific permission for use of Family and Impact.

At Manor House Minster Nursery we use the Family App to communicate with parents and carers and to share information about children's learning and development.

The app stores personal data relating to children and their families, including observations of children's development, photographs, and parent or carer contact details. All information is stored securely and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Access to the app is restricted to authorised staff members and the relevant child's parents or carers. Staff access levels are controlled to ensure that individuals can only view and manage information necessary for their role. Parents and carers can only access information relating to their own child.

Photographs and observations shared through the app are used solely for educational and communication purposes and are handled in line with the nursery's privacy and safeguarding procedures.

In the event of a data breach involving the Family App, the nursery will follow the appropriate procedures and notify all relevant parties as soon as possible. Where required, details of the incident and any recommended actions will be provided.

It is our intention to respect the privacy of children and their families and we do so by:

- Storing confidential physical records in a locked filing cabinet or on the office computer with files that are password protected.
- Access to digital records is password protected, and access is limited to appropriate authorised staff members only.
- Ensuring staff, student and volunteer inductions include an awareness of the importance of confidentiality and that information about the child and family is not shared outside of the nursery other than with relevant professionals who need to know that information. It is not shared with friends and family, or in public places or situations. If staff breach any confidentiality provisions, each case will be looked at individually and the Disciplinary Procedure will be followed. Students on placement in the nursery are given a copy of the Confidentiality Policy and advised that must adhere to the requirements.
- Ensuring that all staff, volunteers and students are aware that this information is confidential and only for use within the nursery and to support the child's best interests with parental permission.
- Ensuring that parents have access to files and records of their own children but not to those of any other child. However if relevant professionals such as the police or local authority children's social care team decide that allowing parents' access is not in the child's best interest than this will be reviewed.
- Ensuring all staff are aware that this information is confidential and only for use within the nursery setting. If any of this information is requested for whatever

reason, the parent's permission will always be sought other than in the circumstances above.

- Ensuring staff, students and volunteers are aware of and follow our social networking policy in relation to confidentiality.
- Ensuring staff, students and volunteers are aware of and follow our social networking policy in relation to confidentiality.
- Ensuring issues concerning the employment of staff remain confidential to the people directly involved with making personnel decisions.
- Ensuring any concerns or evidence relating to a child's personal safety are kept in a secure, confidential file and are shared with relevant people on a need-to-know basis. If however a child is considered at risk, our Safeguarding and Child Protection Policy will override confidentiality.

Procedure for Parents Accessing Their Child's File

Parents may request access to any physical records held on their child and family following the procedure below:

- Any request to see the child's personal file by a parent or person with parental responsibility must be made in writing to the Director Jayne Sheerin.
- The Director informs the relevant manager and sends a written acknowledgement.
- The setting commits to providing access within 14 days - although this may be extended.
- The Manager prepares the file for viewing and the Director approves the file.
- All third parties are written to, stating that a request for disclosure has been received and asking for their permission to disclose to the person requesting it. Copies of these letters are retained on the file.
- Third parties include all family members who may be referred to in the records.
- It also includes workers from any other agency, including social services, the health authority, etc. It is usual for agencies to refuse consent to disclose, preferring the individual to go directly to them.
- When all consents or refusals to disclose have been received these are attached to the copy of the request letter.
- A photocopy of the complete file is taken.
- A manager and the director go through the file and remove any information which a third party has refused consent to disclose. This will be done with a thick black marker, to score through every reference to the third party and information they have added to the file.
- What remains is the information recorded by the setting, detailing the work initiated and followed by them in relation to confidential matters this is a 'clean copy'.
- The clean copy is photocopied for the parents who are then invited to discuss the contents. The file is not given straight over, but checked through by the manager or director, so that it can be explained.
- Legal advice may be sought before sharing a file, especially where the parent has possible grounds for litigation against the setting or another (third party agency).

Any physical photographs (or videos) of the child that are not on the FAMILY app will be handed over /shared with the parent(s) when the child leaves. If we are unable to return this information it will be destroyed/deleted or if required by law kept secure for minimum legal archiving requirement.

Manor House Minster Nursery may hold the following information for employed staff, students, and volunteers:

- Name of staff member
- Email address
- Postal address
- Date of birth
- Marital status
- Bank account details
- Telephone numbers
- National insurance number
- Medical details
- References
- DBS checks
- Declaration of suitability
- Qualifications/Certificates
- ID
- Photos
- Emergency contact name and number
- Disciplinary evidence
- Facial recognition image recording

Personal information is kept secure in a lockable filing cabinet and or on our secure server to which only management have access.

At Manor House Minster Nursery we use the software system Impact Early Years to manage staff information and maintain compliance with regulatory requirements.

The system stores personal data relating to staff, children and parents. All information is stored securely and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Access to the system is restricted through different levels of staff permissions. These access levels ensure that staff members can only view or manage information that is necessary for their job role.

In the event of a data breach, the nursery will follow the appropriate procedures and notify all relevant parties as soon as possible. Where required, we will provide details of the incident and any recommended actions that should be taken.

All staff members and volunteers consent to Manor House Minster Nursery storing this information securely during their induction process.

Individual staff may request to see their own personal file at any time.
When the staff member/volunteer ceases employment with Manor House Minster Nursery all personal data will be destroyed unless required by law to keep secure for the minimum legal requirement.

Safeguarding

Manor House Minster Nursery understands that UK GDPR is not a barrier for sharing information and believe the safety and welfare of a child always comes first.

For child protection purposes children who have been attending the setting where there have been safeguarding concerns will have records transferred to the next educational setting with receipt of transfer. If this is not applicable records will be retained for 25 years, and then destroyed.

The policy will be reviewed annually and amended according to any change in law/legislation.

Manor House Minster Nursery will only share personal information to ensure the child stays safe and healthy or we are legally required to do so.

Manor House Minster Nursery adheres to all data protection guidelines stated in our UK GDPR policy.

NOTE – See Safeguarding policy

Signed on behalf of the nursery	Date for review
Amy Penny April 2025	<i>March 2027</i>