



General Data Protection Regulation Policy

Statement of Intent

The General Data Protection Regulation (GDPR) is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially. This includes both staff and children. How the nursery obtains, shares and uses information is critical, as personal data is sensitive and private. Everyone, adults and children alike, has the right to know how the information about them is used. The General Data Protection Regulation requires the nursery to strike the right balance in processing personal information so that an individual's privacy is protected. Applying the principles to all information held by the nursery will typically achieve this balance and help to comply with the legislation.

We will respect the privacy of children and their parents and carers, while ensuring that they access high quality early years care and education in our setting. We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the General Data Protection Regulation and the Human Rights Act.

General Data Protection Regulation principles

To comply with the act, the nursery must observe the eight 'General Data Protection Regulation principles', ensuring that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In practice, it means that the nursery must:

- have legitimate grounds for collecting and using the personal data.
- not use the data in ways that have unjustified adverse effects on the individuals concerned.
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data.
- handle people's personal data only in ways they would reasonably expect; and
- make sure they do not do anything unlawful with the data

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The General Data Protection Regulation principles apply to all information held electronically or in structured paper files.

The principles also extend to educational records – the names of staff and children, dates of birth, addresses, national insurance numbers, school marks, medical information, SEN assessments and staff development reviews.

Sensitive personal data is information that relates to

- race and ethnicity,
- political opinions,
- religious beliefs,
- membership of trade unions,
- physical and mental health,
- sexuality
- criminal offences

Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a nursery manager may have a nursery e-mail account that is made publicly available on the setting's website whereas their home e-mail account is private and confidential and should only be available to those to whom consent had been granted.

It is important to differentiate between personal information that individuals would expect to be treated as private or confidential (whether legally classified as sensitive personal data) and personal information you can make freely available. For example: the nursery manager's identity

Updated: Sep 22, Jan 23, Sept 24, August 25

is personal information, but everyone would expect it to be publicly available. However, the nursery manager's home phone number would usually be regarded as private information.

What must the nursery do?

- We must notify the ICO (Information Commissioner's Office) that we are processing personal data.
- We have a nominated individual, Nursery Director, as the 'Data Protection Controller'.
- The nursery has clear, practical policies and procedures on information governance for staff to follow, and needs to monitor their operation

These should include:

- Staff Code of Conduct
- Privacy notices for staff and parents/pupils
- Record Management Policy (not mandatory, but good practice)

Data Breaches

In the event of a personal data breach, the Data Protection Controller should be notified immediately and an investigation carried out.

Individual Rights

The General Data Protection Regulation includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The General Data Protection Regulation entitles an individual the right to request the personal information a nursery holds on their behalf – this is known as a Subject Access Request (SAR) and includes all and any information held by the nursery, not just that information held on central

files or electronically, so it could also include correspondence or notes held by others in the nursery.

- SARs must be responded to within 1 month of receipt.
- The SAR should be made in writing by the individual making the request.
- The nursery can refuse or charge for requests that are manifestly unfounded or excessive
- Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

Sharing of data

- Bardfield Montessori maintains records and obtains and shares information (with parents and carers, other professionals working with the child, the police, social services and Ofsted or the childminder agency with which they are registered, as appropriate) to ensure the safe and efficient management of the setting, and to help ensure the needs of all children are met.
- We enable a regular two-way flow of information with parents and/or carers, and between providers, if a child is attending more than one setting.
- When we are informed of a child's attendance at another setting, we will contact the other provider by telephone to confirm attendance and discuss development milestones. Following this, we will create a sharing book for both settings to share so that parents/carers, and setting attended can communicate transparently and share information on development. Sharing books are a positive way to increase communication, share milestones and ensure the needs of the child are met.
- Where data is shared for educational purposes, data is dealt with in upmost confidentiality. When sharing records of a child's development with other professionals, documents will be only accessible through locked files with passwords or delivered by hand to the other professionals by a member of management. This information is then signed by both parties.

Staff Responsibilities

Staff need to know and understand:

- How to manage, keep and dispose of data
- The nursery's procedures in relation to children's records, email, social media, taking photos in the nursery, mobile technology and the nursery website
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

Information and IT Equipment Acceptable Usage

Acceptable Usage covers the security and use of all Bardfield Montessori Ltd information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This applies to all Bardfield Montessori Ltd employees, contractors and agents (hereafter referred to as 'individuals').

Updated: Sep 22, Jan 23, Sept 24, August 25

This applies to all information, in whatever form, relating to Bardfield Montessori Ltd business activities, and to all information handled by Bardfield Montessori Ltd relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Bardfield Montessori Ltd or on its behalf.

Computer Access Control – Individual’s Responsibility

Access to the Bardfield Montessori Ltd IT systems is controlled using User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Bardfield Montessori Ltd IT systems.

Individuals must not:

?? Allow anyone else to use their user ID and password on any Bardfield Montessori Ltd IT system.

?? Leave their user accounts logged in at an unattended and unlocked computer.

?? Use someone else’s user ID and password to access Bardfield Montessori Ltd IT systems.

?? Leave their password unprotected (for example writing it down).

?? Perform any unauthorised changes to Bardfield Montessori Ltd IT systems or information.

?? Attempt to access data that they are not authorised to use or access.

?? Exceed the limits of their authorisation or specific business need to interrogate the system or data.

?? Connect any non-Bardfield Montessori Ltd authorised device to the Bardfield Montessori Ltd network or IT systems

?? Store Bardfield Montessori Ltd data on any non-authorised Bardfield Montessori Ltd equipment.

?? Give or transfer Bardfield Montessori Ltd data or software to any person or organisation outside Bardfield Montessori Ltd without the authority of Play to Learn Ltd.

Managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Updated: Sep 22, Jan 23, Sept 24, August 25

Use of Bardfield Montessori Ltd internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Bardfield Montessori Ltd in any way, not in breach of any term and condition of employment and does not place the individual or Bardfield Montessori Ltd in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

?? Use the internet or email for the purposes of harassment or abuse.

?? Use profanity, obscenities, or derogatory remarks in communications

?? Access, download, send or receive any data (including images), which Bardfield Montessori Ltd considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

?? Use the internet or email to make personal gains or conduct a personal business

?? Use the internet or email to gamble

?? Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

?? Place any information on the Internet that relates to Bardfield Montessori Ltd, alter any information about it, or express any opinion about Bardfield Montessori Ltd, unless they are specifically authorised to do this.

?? Send unprotected sensitive or confidential information externally.

?? Make official commitments through the internet or email on behalf of Bardfield Montessori Ltd unless authorised to do so.

?? Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.

?? In any way infringe any copyright, database rights, trademarks or other intellectual property.

?? Download any software from the internet without prior approval of the IT Department

?? Connect Bardfield Montessori Ltd devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

To reduce the risk of unauthorised access or loss of information, Bardfield Montessori Ltd enforces a clear desk and screen policy as follows:

Updated: Sep 22, Jan 23, Sept 24, August 25

Personal or confidential business information must be protected using security features provided for example secure print on printers.

Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

Care must be taken to not leave confidential material on printers or photocopiers.

All business-related printed matter must be disposed of using confidential waste bins or shredders.

- Staff must upload photos to the online record keeping programme and clear photos from iPad storage regularly.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

Working away from the office must be in line with Bardfield Montessori Ltd remote working policy.

Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.

Laptops must be carried as hand luggage when travelling.

Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.

Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Bardfield Montessori Ltd authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorised by Bardfield Montessori Ltd on Bardfield Montessori Ltd computers. Authorised software must be used in accordance with the software

Updated: Sep 22, Jan 23, Sept 24, August 25

supplier's licensing agreements. All software on Bardfield Montessori Ltd computers must be approved and installed by Bardfield Montessori Ltd IT support.

Individuals must not:

?? Store personal files such as music, video, photographs or games on Bardfield Montessori Ltd IT equipment

Viruses

The IT support has implemented centralised, automated virus detection and virus software updates within the Bardfield Montessori Ltd. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

?? Remove or disable anti-virus software

?? Attempt to remove virus-infected files or clean up an infection, other than using approved Bardfield Montessori Ltd anti-virus software and procedures.

Telephony (Voice) Equipment Conditions of Use

Use of Bardfield Montessori Ltd voice equipment is intended for business use. Individuals must not use Bardfield Montessori Ltd voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

?? Use Bardfield Montessori Ltd voice for conducting private business.

?? Make hoax or threatening calls to internal or external destinations

?? Accept reverse charge calls from domestic or international operators, unless it is for business use

Actions upon Termination of Contract

All Bardfield Montessori Ltd equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Bardfield Montessori Ltd at termination of contract.

All Bardfield Montessori Ltd data or intellectual property developed or gained during the period of employment remains the property of Bardfield Montessori Ltd and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on Bardfield Montessori Ltd computers is the property of Bardfield Montessori Ltd and there is no official provision for individual data privacy, however wherever possible Bardfield Montessori Ltd will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Bardfield Montessori Ltd has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the

Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

It is your responsibility to report suspected breaches of security policy without delay to the management team.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Bardfield Montessori Ltd disciplinary procedures.

Access to staff personal data

- Employees are allowed to have access to all personal data about them held on manual or computer records under the Data Protection Act (1998). The Act requires the organisation to action requests for access to personal data within one month.
- Should an employee request access to their personal data, the request must be addressed in writing to the relevant line manager. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will be informed whether or not the request is to be granted. If it is, the information will be provided within one month of the date of the request.

- In the event of a disagreement between an employee and the line manager regarding personal data, the matter should be taken up under the charity's grievance procedure.
- The right of employees to see information held about them is extended to information held in paper record-keeping systems as well as computerised systems.
- There are some exemptions; for example, employees will not be able to see employment references about them supplied in confidence, nor will people involved in negotiations with the data controller be able to see information about the data controller's intentions in relation to those negotiations.
- Employee data cannot be used for direct marketing (including fundraising) if the data subject objects. Approval to use employee data for marketing purposes must be sought from the Director of Communications.

Legal Framework

General Data Protection Regulation 2018 <https://ico.org.uk/>

Data Protection Act 1998

Computer Misuse Act 1990

Freedom of Information Act 2000

Human Rights Act 1999

The Children Act 2004, 2006 (Every Child Matters)

Statutory Framework

Statutory Framework for the Early Years 2025

Section 3: The Safeguarding and Welfare requirements 3.6 – 3.8

Nursery Policies:

Child Protection

E-safety