**9 (A)** **DATA PROTECTION POLICY (GDPR)**

**Statement of Intent**

The General Data Protection Regulation (GDPR) Act came into effect on 25th May 2018. It 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 pre-school 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 pre-school 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 pre-school 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 pre-school 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.

**The GDPR offers six lawful bases** for processing personal information. These are the only justifications for doing so. They are:

* necessary to enter into or to perform a contract,
* necessary for compliance with a legal obligation,
* necessary to protect ‘vital interests’,
* necessary for the public interest,
* necessary for a legitimate interest,
* with the consent of the data subject.

 The ICO says that consent should generally be considered the last resort, if no other justification applies. In practice, it means that the pre-school 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, development records, medical information, SEND 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 pre-school manager may have a pre-school e-mail account that is made publicly available on the school’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 pre-school manager’s identity is personal information, but everyone would expect it to be publicly available. However, the pre-school manager’s home phone number would usually be regarded as private information.

**The personal data we hold**

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

* Contact details, contact preferences, date of birth, identification documents
* Pupil and curricular records
* Characteristics, such as ethnic background, eligibility for 2 year old funding or special educational needs
* Exclusion/Inclusion information
* Details of any medical conditions, including physical and mental health
* Attendance information
* Safeguarding information
* Details of any support received, including care packages, plans and support providers
* Photographs

**Purposes’ for which personal data can be held. (Staff)**

Personal data relating to employees may be collected for the purposes of -

* Safer recruitment, Promotion, training, or deployment, and/or career development
* Administration and payments of wages
* Calculations of certain benefits including pensions
* Disciplinary or performance management purposes:
* Performance reviews
* Recording of communication with employees and their representatives
* Compliances with legislation
* Provision of references of financial institutions, to facilitate entry onto educational courses and/or to assist potential employers:
* Staffing levels and career planning

The company considers that the following personal data falls within the categories set out above:

* Personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origins and nationality will also be deemed as relevant.
* References, CV and up to date DBS check number and date checked.
* Emergency contact details
* Appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment:
* Training records
* Salary, benefits and banking/building society details
* Absences and sickness records (signing in and out records)

Employees or potential employees will be advised by the company of the person data which has been obtained or retained, its source and the purposes for which the personal data may be used or to whom it will be disclosed.

**Purposes’ for which personal data can be held (children and families)**

Personal data relating to children and their families may be collected for the purposes of

* Communication between approved outside agencies such as early years and education in the local authorities, OFSTED and social services.
* Administration and payment charts
* Invoices and calculation of fees
* Communication with parents, key workers, recognised outside agencies and other childcare providers
* Children profiles to develop and record children’s development.
* Recorded communications with staff and parents including complaints.
* All records that ensure the safe guarding of the individual children including accident records, incidents and medication records.
* Records of reports outlining children’s development.
* Compliance with legislation.

**What must the pre-school do?**

* We must notify the ICO (Information Commissioner’s Office) that we are processing personal data.
* We have a nominated individual, as the ‘Data Protection Officer’.
* The pre-school 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

**Responsibility for the processing of personal data**

The company has a designated Data Protection Officer. This person is responsible for ensuring all personal data is controlled in compliance with the GDPR act 2018.

Employees who have access to personal data must comply with this policy and adhere to the procedures laid down by the Data Protection Officer.

Failure to comply with the policies and procedure may result in disciplinary action up to and including suspension or dismissal.

**Use of personal Data**

To ensure compliance with GDPR Act 2018 and the interest of privacy, confidence and good employee and parent relations, the disclosure and use of information held by the company is governed by the following conditions.

* Personal data must only be used for one or more purpose specified in this policy.
* Company documents may only be used in accordance with the statement within each document stating its intended use:
* Provided that identification of any individual is not disclosed aggregate or statistical information may be used to respond to any legitimate internal or external request for data e.g. surveys staffing level figures)
* Personal data must not be disclosed either within or outside the company to any unauthorised recipient.

**Personal Data held for equal opportunities monitoring purposes**

 Where personal date obtained about candidates is to be held for the purpose of equal opportunities monitoring, all such data must be made anonymous.

**Disclosure of personal data and Data Sharing**

Personal data may only be disclosed outside the company with the written consent of parents or the employee in question, where disclosure is required by law or where there is immediate danger to staff member, parent or a child in the Pre-school.

 We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information with:

* Our local authority- to meet our legal obligations to share certain information with it, such as safeguarding concerns.
* The department of Education
* The child’s family and representatives
* Our regulators e.g. Ofsted
* Suppliers and service providers- to enable them to provide the service we have contracted them for.
* Financial Organisations
* Central and local government
* Our auditors
* Survey
* Health authorities
* Security Organisations
* Health and social welfare organisations
* Professional advisers and consultants
* Police forces, courts, tribunals
* Professional bodies
* Charities and voluntary organisations

**Slough Early Years Portal**

We are required to provide information about children to Slough early years through their portal for the funding, census, data collection and attendance purposes.

**Transferring data internationally**

Where we transfer personal data outside the country or, we will do in accordance with data protection law.

**How we store this data**

We keep personal information about children while they are attending Little Diamonds Preschool. We may also keep it beyond their attendance at our Preschool if this is necessary to comply with our legal obligations.

**Retention Period of records**

We will adhere to the legal requirements on retention periods for records. In addition, we will endeavour to follow the recommended guidelines where possible and practical. Please read Retention Period for records and GDPR data audit for more information.

**Parent’s and children’s rights regarding personal data**

Individuals have a right to make a ‘Subject access request’ to gain access to personal data the Preschool holds about them
Parents/carers can make a request with respect to their child’s data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12)

Parents also have the right to make a request to access data the Preschool holds about them

If you make a request, and if we do hold any information about you or your child, we will:

* Give you a description of it
* Tell you why we are holding and processing it and how long we will keep it for.
* Explain where we got it from, if not from you or your child.
* Tell you who it has been, or will be, shared with
* Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
* Give you a copy of the information.

Individuals have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

Request can be made in writing by contacting our data protection officer.

**Other rights**

Under data protection law, individuals have certain rights regarding the personal data is used and kept safe, including the right to:

* Object to use of personal data if it would cause or is causing damage or distress.
* Objects to the decisions being taken by automated means e.g. computer or machine.
* Prevent it being used to send direct marketing
* In certain circumstances, have inaccurate personal data corrected, deleted, or destroyed or restrict processing.
* Claim compensation for damages caused by a breach of the data protection regulations.

**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) and GDPR act. 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.
* 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.
* 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 in the form of written consent.

**Accuracy of personal data**

The company will review personal date regularly to ensure that it is accurate, relevant and up to date. To ensure the company files are accurate and up to date, and so that the company is able to contact the employee/parent or in the case of an emergency another designated person. Employees/parents must notify the company as soon as possible of any changes in their personal details (e.g. home address, telephone numbers, and emergency contact details)

Standard printouts will be issued to staff on an annual basis for ensuring that data is up to date and accurate. Employees/ parents are entitled to amend any incorrect details and these corrections will be made to all files held on the company’s information system.

In some cases, documentary evidence such as qualification certificates will be requested before any changes are made.

Once completed, these records will be stored in the employees personnel file or child’s detail file.

**Staff Responsibilities**

Staff need to know and understand:

* How to manage, keep and dispose of data
* The pre-school’s procedures in relation to children’s records, email, social media, taking photos in the pre-school, mobile technology and the pre-school 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 Little Diamonds Preschool information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This applies to all Little Diamonds Preschool employees, contractors and agents (hereafter referred to as ‘individuals’).

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

**Computer Access Control – Individual’s Responsibility**

Access to the Little Diamonds Preschool IT systems is controlled by the use of 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 Little Diamonds Preschool IT systems

**Individuals must not:**

* Allow anyone else to use their user ID and password on any Little Diamonds Preschool IT system
* Leave their user accounts logged in at an unattended and unlocked computer.
* Use someone else’s user ID and password to access Little Diamonds Preschool IT systems
* Leave their password unprotected (for example writing it down).
* Perform any unauthorised changes to Little Diamonds 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-Little Diamonds Preschool authorised device to the Little Diamonds Preschool network or IT systems
* Store Little Diamonds data on any non-authorised equipment
* Give or transfer Little Diamonds Preschool data or software to any person or organisation outside without the authority of Little Diamonds Preschool.

Pre-school 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**

Use of 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 Little Diamonds Preschool in any way, not in breach of any term and condition of employment and does not place the individual or Little Diamonds Preschool 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 Little Diamonds Preschool 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 Little Diamonds Preschool, alter any information about it, or express any opinion about Little Diamonds Preschool, 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 Little Diamonds Preschool 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 Little Diamonds Preschool devices to the internet using non-standard connections

**Clear Desk and Clear Screen Policy**

In order to reduce the risk of unauthorised access or loss of information, Little Diamonds Preschool enforces a clear desk and screen policy as follows:

* 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.

**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 Little Diamonds Preschool guidelines.
* 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 Little Diamonds Preschool 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 Little Diamonds Preschool on Little Diamonds Preschool computers. Authorised software must be used in accordance with the software supplier's licensing agreements.

**Viruses**

The IT support has implemented centralised, automated virus detection and virus software updates within the Little Diamonds Preschool. 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 by the use of approved Little Diamonds Preschool anti-virus software and procedures.

**Telephony (Voice) Equipment Conditions of Use**

Use of Little Diamonds Preschool voice equipment is intended for business use. Individuals must not use Little Diamonds Preschool 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 Little Diamonds Preschool 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

**Monitoring and Filtering**

All data that is created and stored on Little Diamonds Preschool computers is the property of Little Diamonds Preschool and there is no official provision for individual data privacy, however wherever possible Little Diamonds Preschool 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. Little Diamonds Preschool has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order 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

**The company will review the nature of the information being collected and held on a yearly basis.**

**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

Section 3: The Safeguarding and Welfare requirements 3.67-3.72

Policy Revised on March 2021