GENERAL DATA PROCESSING REGULATIONS (GDPR)
POLICY AND PROCEDURES

We are registered with the ICO (Information Commissioners Office)

TABLE OF CONTENTS

GDPR – GENERAL DATA PROTECTION REGULATION

GDPR came into effect on 25 May 2018, and it replaced current the Data Protection Act (DPA) legislation. It is intended to provide greater transparency around the collection and use of data. The scheme will be governed by the Information Commissioner's Office (ICO).

GDPR states that personal data should be 'processed fairly & lawfully' and 'collected for specified, explicit and legitimate purposes' and that individual's data is not processed without their knowledge and are only processed with their 'explicit' consent.

Our nursery aims to ensure that all personal data collected about staff, children, parents, carers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format. The six principles of GDPR are that data is:

1. Processed fairly, lawfully and in a transparent manner
2. Used for specified, explicit and legitimate purposes
3. Used in a way that is adequate, relevant and limited
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed in a manner that ensures appropriate security of the data

Under GDPR people will continue to have the right to a Freedom of Information request (FOI) – from bodies dealing with public money or a Subject Access Request (SAR) - anyone can request data from anyone else.

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras CCTV and personal information.

COMMON GDPR DEFINITIONS

Personal data

Any information either digital or hard copy relating to an identified, or identifiable, individual. This may include the individual's name (including initials), address, phone number, online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, health – physical or mental, sexual orientation.

Processing
Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject
The identified or identifiable individual whose personal data is held or processed.

Data controller
A person or organisation that determines the purposes and the means of processing of personal data.

Data processor
A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

OUR OBLIGATIONS FOR GDPR

- ICO - Our nursery is registered with the ICO (Information Commissioners Office). Our current certificate is on display in the entrance hallway.
- Individual rights — Our nursery acknowledges that individuals will have new and enhanced rights on the collection, access and erasure of their data. We will ensure our nursery has systems and processes in place that promotes these rights.
- Privacy notices — When we collect any data we will be transparent by informing people how we are going to use it, who we may share it with, how long we will keep it.
- Consent — Whilst we have legitimate legal reasons for collecting and processing personalised data, we will ask for your consent for a range of activities and data processing so that we and you are able to evidence consent was freely given.
- Data agreements — We will have written arrangements with external organisations such as Sheffied City Council if they are processing data for us, such as EYFEL. We will ensure that anyone processing data on our behalf will be compliant with the GDPR requirements.
- Appointing a data protection officer —The Nursery Proprietor will be the Designated Data Controller supported by the Nursery Managers. The Nursery Proprietor will be the person who takes the lead on data compliance within the nursery and to ensure compliance with GDPR.
- Breach notification — We acknowledge our obligation to notify the Information Commissioners Office (ICO) of any data breach within 72 hours of becoming aware of the breach.
- Penalties — We acknowledge that failure to comply with GDPR obligations may result in heavy penalties for each data breach.

UPHOLDING GDPR RIGHTS – OUR APPROACH

GDPR provides rights for all parties concerned with the creation, storage and sharing of data and our nursery fulfils our obligations under these rights as follows:

<u>The Right to be Informed</u>
Our nursery is registered with Ofsted and the Local Authority and consequently, is required to collect and manage certain data, such as:

- Parent's/Carer's names, addresses, telephone numbers, email addresses, bank details, date of birth and National Insurance numbers.
- We need to know children's' full names, addresses, date of birth and Birth Certificate number, plus other information relating to their health and well-being as contained in our care plan. For parents claiming the free nursery entitlement we are requested to provide this data to Sheffield City Council; this information is sent to the Local Authority via a secure electronic file transfer system.
- We are required to collect certain details of visitors to our nursery. We need to know visits names, telephone numbers, addresses and where appropriate company name. This is in respect of our Health and Safety and Safeguarding Policies.
- As an employer we are required to hold data on our employees; names, addresses, email addresses, telephone numbers, date of birth, National Insurance numbers, photographic ID such as passport and driver's license, bank details.
- Information is also required for Disclosure and Barring Service checks (DBS) and proof of eligibility to work in the UK. This information is sent via a secure file transfer system to our provider for the processing of DBS checks.
-

The Right of Access

At any point an individual can make a request relating to their data and we will need to provide a response (within 1 month). We can refuse a request, if we have a lawful obligation to retain data i.e. from Ofsted in relation to the EYFS, but we will inform the individual of the reasons for the rejection. The individual will have the right to complain to the ICO if they are not happy with the decision.

The Right of Erasure or Deletion

You have the right to request the deletion of your data where there is no compelling reason for its continued use. However, our nursery has a legal duty to keep children's and parents details for 3 years after leaving nursery. Staff records must be kept for 6 years after the member of staff leaves employment, before they can be erased. This data is archived securely and shredded after the legal retention period.

The Right to Restrict Processing

Parents, visitors and staff can object to our nursery processing their data. This means that records can be stored but must not be used in any way, for example reports or for communications. If the restriction does not enable us to perform our childcare service, we will consult with the requester to find an acceptable solution. If none can be found then the childcare service may be discontinued.

The to Data Portability

Our nursery requires data to be transferred from one IT system to another; such as from The Learning Journals to the Local Authority, to other settings, to Nursery Manager. These recipients use secure file transfer systems and have their own policies and procedures in place in relation to GDPR.

The Right to Object

Parents, visitors and staff can object to their data being used for certain activities like marketing or research.

The Right Not to be Subject to Profiling or Automated Decisions

Automated decisions and profiling are used in marketing based organisations. Our nursery does not use or share personal data for such purposes.

COLLECTING PERSONAL DATA

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the nursery can fulfil a contract with the individual, or the individual has asked the nursery to take specific steps before entering into a contract.
- The data needs to be processed so that the nursery can comply with a legal / Ofsted obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that the nursery can carry out its official functions.
- The data needs to be processed for the legitimate interests of the nursery or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of an enrolled child at the nursery) has freely given clear consent.

SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/ carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to us – for example, IT companies. When doing this, we will only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.

SUBJECT ACCESS REQUESTS TO THE NURSERY - ADULTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the nursery holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or the criteria used to determine this period.
- The source of the data, if not the individual.

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing via nursery email.

SUBJECT ACCESS REQUESTS TO THE NURSERY - CHILDREN

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from our parents or carers will be considered without the express permission of the child.

RESPONDING TO SUBJECT ACCESS REQUESTS

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

CCTV

We use CCTV in various locations around the nursery to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the Designated Data Controller.

PHOTOGRAPHS AND VIDEOGRAPHY

As part of our nursery activities and as part of your child's learning profile, we may take photographs and record images of individuals and / or children. We will obtain written consent from parents and carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to the parent and carer. Authorised uses may include:

- Within the nursery on notice boards, pegs, observations, etc.
- Outside of nursery by external agencies such as a nursery appointed photographer.
- Online on our nursery website or Learning Journal systems.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

STORAGE OF PAPER OR DIGITAL INFORMATION / MEDIA

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- All paper copies of children's and staff records are kept in a locked office and locked filing cabinets in our nursery. Members of staff can have access to these files but information taken from the files about individual children is confidential and apart from archiving, these records remain on site at all times. These records are shredded after the retention period.
- Papers containing confidential personal data will not be left on office desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the nursery office.
- Passwords will be at least 8 characters long containing letters and numbers are used to access nursery computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals.
- Encryption software will be used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff who store personal information on their personal devices (phones) are expected to follow the same security procedures as for school-owned equipment (as per our acceptable use policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

DISPOSAL OF DATA

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the nursery's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

DATA AUDIT AND PROCEDURE

To ensure our nursery is complying with GDPR a full data audit will be conducted every 2 years to ensure that there is a valid reason to hold data, that permission to hold all data has been sought and that the risk of data breaches is minimised.

- Find and record all documents either paper and/or on computer that contain information identifying a person / child, whether shared or not.

- Print off one copy of the relevant document and complete the data audit sheet.

- Identify if (1) the document can be deleted (2) the document can archived and for how long (3) the document is current. (4) the document needs updating.

During the Data Audit it is necessary to make sure that we have consent for every piece of data held – if there is no specific permission this must be gained if the data is to be kept.

KEY NURSERY AREAS TO BE AUDITED

There are many areas within the nursery that contain both paper and digital data and these need to be assessed for validity, security and compliance:

- Learning journal software
- Microsoft Office
- Microsoft Outlook for email
- Booking and enquiry forms
- Children's files
- Records of allergies – in files and in rooms
- Child Protection/Safeguarding information
- EYFE funding information
- Attendance records
- Staff files
- Contact cards
- Information held in rooms

- Information on hardware; computers, iPads, laptops – portable devices should not be removed from the data controller premises unless encrypted, PCs need to be locked every time user leaves their desk
- Information stored in office desks or shelves must be secure if it holds personal data
- Information held in remote offices (or at home if portable device taken from controller premises) – access to these by people not entitled to view it, i.e. anyone in the household must be restricted by secure systems/processes.

STAFF RESPONSIBILITIES

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the nursery of any changes to their personal data, such as a change of address.

Staff should contact the designated data controller (Nursery Proprietor) in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure - if they have any concerns that this policy is not being followed.
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals - if they need help with any contracts or sharing personal data with third parties.

DATA BREACH – PROCEDURE

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Designated Data Controller (DDC ~ Nursery Proprietor).

- The DDC will investigate the report and determine whether a breach has occurred. To decide, the DDC will consider whether personal data has been accidentally or unlawfully: - lost - stolen - destroyed - altered - disclosed or made available where it should not have been - made available to unauthorised people.
- The DDC will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
- The DDC will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DDC will work out whether the breach must be reported to the ICO.
- The DDC will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

- Where the ICO must be notified, the DDC will do this via the 'report a breach' page of the ICO website within 72 hours.
- The DDC will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DDC will promptly inform, in writing, all individuals whose personal data has been breached.
- The DDC will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DDC and nursery management team will meet to review what happened and how it can be prevented from happening again.

DATA RETENTION – TIMESCALES

Children's records including registers medication, accident books	3 years after child has left
Child protection and safeguarding records	Until the child is 24
Records of reportable injuries, death, disease or dangerous occurrence	3 years after the record was made
Staff files, training, disciplinary, time sheets	6 years after employment ceases
DBS Checks	6 months
Wages and salary records	6 years
Statutory Maternity records	3 years to the end of the tax year to which they relate
Statutory Sick Pay	3 years to the end of the tax year to which they relate
Income tax and National Insurance records	3 years to the end of the tax year to which they relate
Redundancy details	6 years after employment ends
Staff accident records and RIDDOR	3 years after record made
Accident/medical records as specified by COSHH	40 years from the date of the last entry
Accounting records	3 years to the end of the tax year to which they relate
Employers Liability Insurance	As long as possible