SCORTON VILLAGE PRE-SCHOOL

POLICIES AND PROCEDURES

Data Protection and Confidentiality

Data Protection and Confidentiality

CONTENTS

1. INTRODUCTION

Related policies and procedures

This policy is to be read in conjunction with Scorton Village Pre-School's Safeguarding policies.

Representatives

Scorton Village Pre-School committee along with the staff are responsible for data protection.

2. DATA PROTECTION POLICY

We keep records and documentation for the purpose of maintaining our Pre-School. Our records are kept in accordance with legal requirements and in accordance with our Data Protection, Data Security and Confidentiality policies. These include:

- Children's Records
    - Developmental records
    - Personal Records
- Pre-School Records
    - Employment Records
    - Child Protection Documentation
    - Financial Records
    - Health and Safety Documentation
    - Business/Charity Records

Data Protection Principles

The GDPR requires that all personal data is:

- Processed lawfully, fairly in a transparent manner in relation to individuals
- Collected for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccuracies are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Scorton Village Pre-School as a data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Personal Data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Sensitive Personal Data

The GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include ethnic origin, race, religion, genetic data, and biometric data where processed to uniquely identify an individual.

Lawful Bases and Specific Conditions for Processing Data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

The specific conditions of processing special category data are set out in Article 9(2) of the GDPR https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Our Privacy Notices detail the Lawful Bases and Specific Conditions we will use for processing data.

Where we require consent, a consent form will be issued. Once granted consent may be withdrawn by contacting Pre-School. Please note that all processing of your personal data will cease once you have withdrawn consent, but this will not affect any personal data that has already been processed prior to this point.

Individual Rights

The GDPR provides 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
- Rights in relation to automated decision making and profiling.

The lawful basis for your processing can also affect which rights are available to individuals. For example:

- The right to erasure does not apply to processing on the basis of legal obligation or public task.
- The right to portability only applies to processing on the basis of consent or contract.
- The right to object only applies to processing on the basis of public task or legitimate interests.

If any of the above rights are exercised we will respond within 28 days of the request.

Full information can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Under data protection legislation, individuals have the right to request access to information about them that we hold. To make a Subject Access Request, contact the Pre-School Leader using the Subject Access Request Form.

3. Data Security Policy

Scorton Village Pre-School committee is responsible for the management of the setting including the safe storage of personal data. Together with the Pre-School staff they will ensure the highest level of security is maintained at all times.

All staff will be trained on data protection. Staff will be supported to promote a positive culture towards data protection legislation and compliance.

An Information Asset Register of all personal data will be kept detailing what it is, where it is kept and retention periods. We will also list who we share information with. A destruction record will also be kept.

Privacy notices will be issued to all users and staff of Pre-School. These detail what information we will collect and how we use it. Consent forms will also be issued when we require them.

Personal paper records are kept in a secure cabinet, only authorised persons will be permitted to access. In agreement with management and when parental consent is granted learning journey files may be updated at the home of the key person. Greatest care will be taken to ensure the safe storage of the files both in transit and at the property of the staff member.

Electronic data stored on Pre-School devices is password protected, with only authorised persons permitted access. The devices will be kept in a safe area, and the building is secured when not in use with known limited key holders. In agreement with management and NYCC the devices may be used at the home of a member of staff. Greatest care will be taken to ensure the safe storage of the device both in transit and at the property of the staff member.

Access to personal data records will only be permitted to those with parental responsibility of the specific child.

Photographs are only taken in accordance with out Mobile Phone and Camera Policy. Use of the photographs is detailed within our Privacy Notices and Consent Forms.

Pre-School coat pegs are in a public area of the building and are named. Written parental consent will be sought to use child's first name on coat peg. No other identifying information is to be permitted.

4. Confidentiality

Staff will only discuss an individual child with the parents/carers of that child. In certain circumstances information may be released to emergency contacts or collecting adults when it is in best interests of the child. We will also notify parents of this information at the earliest opportunity.

Any information given by parents to our staff will be treated as confidential. Consent will be sought if we feel this information needs to be shared.

Any anxieties/evidence relating to a child's personal safety will be kept confidential and shared with the Designated Safeguarding Lead Practitioner/Pre-School Leader and the Chairperson. Information will only be shared with other staff on a need to know basis.

Staff issues, whether employed or voluntary, will remain confidential to the people directly involved with making personnel decisions.

Pre-School takes a professional approach to confidentiality and the privacy of family life. Our policy is that staff do not make or accept invitations to become online friends with parents or other family carers on any social networking site. This policy also applies to all students. A standard response to decline invitations is available.

Facebook, Twitter, other social networking sites or personal blogs are a public form of communication. In their non-working time, staff and students remain responsible for taking care not to post anything online that breaks confidentiality about children, families or colleagues, or that could damage the reputation of Pre-School. Parents will be discouraged from private messaging any staff member. Advice from the Designated Safeguarding Lead Practitioner will be sought if this occurs.

Scorton Village Pre-school has a Mobile Phone and Camera Policy. Staff, students, volunteers or visitors are reminded of this.

Information Asset Register

We will keep a register of all information we hold. This will include:

- Descriptions of the data
- The form in which we hold it
- Where it is stored
- If we share the information and who with
- If the information contains personal details
- The retention period

If our documentation contains differing retention periods to the information asset register the longer period will apply until the retention period is clarified.

Destruction of Data

This will only be done once retention period has elapsed.

Documentation will be destroyed using a cross cut shredder.

If a third party company is hired to do this, a confidentiality agreement will be signed and if possible destruction will be witnessed by a member of staff.

A Destruction Register will be kept to prevent legitimately destroyed data being considered lost.

Breach of Personal Data

A breach of personal data means a breach in 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.

If a breach of personal data occurs, we will complete a Personal Data Breach Report form. We will establish the likelihood and severity of the resulting risk to the person's rights and freedoms. If it is unlikely there will be a risk we will take internal measures to prevent a breach occurring again. If there is a risk is found we will notify the ICO within 72 hours of becoming aware of the breach. When reporting a breach to the ICO, we must provide:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of a contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible to allow individuals to take steps to protect themselves from the effects of the breach.