Data Protection and Sharing Information Policy

Purpose of Policy

To ensure that where information is stored or processed steps are taken to ensure that this information is stored or processed in accordance with the General Data Protection Regulation (2018). St Michael's Church Pre-School and Nursery is committed to keeping personal information about children, parents, carers and staff as secure as possible and will only share information if it relates to public interest, i.e. prevent crime or harm or if the outcome of not sharing could be worse than having shared it.

Our Commitment

At St Michael's Church Pre-School and Nursery we will only collect information that is necessary for what we do. We will be fair in the way we collect information about you. We will tell you what we intend to do with the information about you. Where practicable, we will collect information directly from you. If we collect information about you from someone else, we will make sure you know that we have done this whenever possible.

Who is Responsible?

It is the responsibility of all members of staff to ensure that personal information about children, parents, carers and colleagues is not shared with individuals outside the setting. All staff have the responsibility to ensure that all personal information is kept safe and secure, and in compliance with the Data Protection Act 1998 and General Data Protection Regulation.

Keeping Information up to date

We will make sure the information about you is accurate and up to date when we collect it. It is your responsibility to keep us informed of any changes of information we hold about you. We will hold information about you and your child for as long as the law says. After this, we will dispose of it securely.

What Personal information we hold;

- Children's details such as name, address, date of birth, room, and medical information.
- Parents/carers information such as name, address, telephone numbers, and bank details.
- Staff information such as name, address, telephone numbers, bank details, national insurance number and qualifications.

Other information including without limitation to:

- Children's developmental journal
- Children protection logs
- Accident and incident Records
- Restraint Records
- Administration of Medication Records
- S.E.N.D. Records
- Legal Records/ Court Orders

Storage of information

We will keep information about you and your child secure. We will protect information against unauthorised change, damage, loss or theft.

Information is stored in two forms:

1. Paper: paper copies of personal information are stored in a locked cupboard or cabinet which has limited access to staff members and no access for parents/carers. Parents/carers should feel secure that the information about their children is not accessible to anyone apart from themselves and setting staff.
2. Computer: any information that is stored on computer will be held in accordance with the Data Protection Act 2018 and General Data Protection Regulation (2018). Access to information stored on computer is limited to staff members, all setting computers are password encoded and only staff members are in possession of the password. Passwords are changed at regular intervals to keep all data protected.

Gaining Consent

- Our policies and procedures set out our responsibility regarding gaining consent to share information and when it may not be sought or overridden.
- We may cover this verbally when the child starts or include this in our prospectus.
- Parents/carers sign a form at registration to give their consent. Parent's /carers have a right to withdraw their consent at any time and can do so in writing.
- Parents/carers are asked to give written consent to share information about any additional needs their child may have, or to pass on child development summaries, to the next provider/school.

Sharing Information

St Michael's Church Pre-School and Nursery recognises that parents/carers have a right to know that the information they share will be regarded as confidential, as well as being informed about the circumstances, and reasons, when we are obliged to share information.

We are obliged to share confidential information without authorisation from the person who provided it or to whom it relates, if it is in the individual's interest. That is when:

- It is to prevent a crime from being committed or intervene where one may have been, or to prevent harm to a child or adult.
- Not sharing it could be worse than the outcome of having shared it.

- The decision should never be made as an individual, but with the back-up of management. The three critical criteria are:

    1. Where there is *evidence* that the child is suffering, or is at risk of suffering, significant harm.
    2. Where there *is reasonable cause to believe* that a child may be suffering, or at risk of suffering, significant harm.
    3. To *prevent* significant harm arising to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime.

We consider the following questions when we need to share:

- Is there a legitimate purpose to sharing the information?
- Does the information enable the person to be identified?
- Is the information confidential?
- If the information is confidential, do you have consent to share?
- Is there a statutory duty or court order to share information?
- If consent is refused, or there are good reasons not to seek consent, is there sufficient public interest to share information?
- If the decision is to share, are you sharing the right information in the right way?
- Have you properly recorded your decision?

All the undertakings above are subject to the paramount commitment of our Pre-School and Nursery, which is to the safety and well-being of the child. Please also see our Safeguarding Children and Child Protection policy.

Breaches to data

Breaches in data will need to be notified to the ICO if the individual could suffer some form of damage such as identity theft, discrimination, and damage to reputation, loss of confidentiality, financial loss or any other significant social disadvantage.

Parental rights

- You have a right to be informed of how we process data and the period we retain data.
- You have a right to access any data we hold on you or your family and right to know if we make adjustments to this data
- You have a right to know where we send yours and your families data
- You have a right to object to us sharing/ storing information if it is not for legal reasons and a right to opt in.
- You have a right to withdraw your consent on the holding of data or remove data if it is not needed for legal reasons.

Raising complaint

If you are concerned about how we hold your data please contact the management team. If you wish to complain externally, as a parent or carer you have a right to complain to the ICO (Information Commissioner's Office) if you think there is a problem with the way the Pre-School and Nursery is handling your data.

Legal framework

- Data Protection Act 2018
- Human Rights Act 1998
- General Data Protection Regulation (GDPR)
- Freedom of Information Act (2014)

Famly Use

At the Pre-School and Nursery we recognise that parents and carers have very busy lives. We therefore want to make it as easy as possible for you to access information about your child's time at the Pre-School and Nursery and also be able to give us information from home. We believe using an online learning journal will make this easier for parents and carers.

- Parents/Carers permission will be gained for photos and recordings of their child to be used on the tapestry app and within other children's Famly profiles.
- Parents will confirm that they will not share photos from tapestry e.g. online, texts, email, social networking. If permission is not gained, staff members will be informed and a paper learning journal will be used.
- Your child's learning journal can be accessed via https://www.famly.co/ or by downloading the app.
- Each individual's child's learning journal is stored securely on the family database and can only be accessed using a unique password which will be given to the parent/carer.
- Staff members will use famly via tablets which we be stored securely in a locked cabinet.
- Staff will not share their passwords with others and will not access the famly app outside the workplace without prior permission.
- Staff will not share the famly app with others outside of the workplace.
- Staff members who access famly outside the setting must do so on secure network and they must have an anti-virus installed