10.10 Maidenbower Pre-School Playgroup

Safeguarding and Welfare Requirement: Information and Records

Providers must maintain records and obtain and share information to ensure the safe and efficient management of the setting, and to help ensure the needs of all the children are met.

General Data Protection Regulation Policy and Information Sharing

"sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals lives. It could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. At the other end of the spectrum, it could be the difference between life and death." (HM Government 2015)

Introduction.

Maidenbower Pre-School Playgroup needs to gather and use certain information about individuals.

These can include parents/carers and children (data subjects) committee members, employees and suppliers, business contacts and other people the playgroup has a relationship with or may need to contact (third parties)

This policy describes how this personal data must be collected, handled and stored to meet the playgroups data protection standards and to comply with the law.

Why this policy exists.

This GDPR and Information Sharing Policy ensures Maidenbower Pre-School Playgroup:

- Complies with data protection law and follows good practice.
- Protects the right of staff, parents/carers, children, committee and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risk of a data breach.

Data protection law.

The Data Protection Act 1998 describes how organisations including Maidenbower Pre-School Playgroup must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

We recognise that parents have a right to know that the information they share with us will be regarded as confidential, as well as to be informed about the circumstances when, and the reasons why, we are obliged to share information.

We record and share information about children and their families (data subjects) in line with the six principles of the General Data Protection Regulation (GDPR) (2018) which are further explained in our Privacy Notice, that is given to parents in their Welcome Pack at the point of registration. The six principles state that personal date must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purpose for which data is processed.
4. Accurate and where necessary, kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purpose for which data is processed.
6. Processed in a way that ensures appropriate security of the personal data including protection against accidental loss, destruction or damage. Using appropriate technical or organisational measures.

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 public interest. That is when:

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

The responsibility for decision-making should not rely solely on an individual but should have the back-up of the management team. The management team provide clear guidance, policy and procedures to ensure all staff and volunteers understand their information sharing responsibilities and are able to respond in a timely, appropriate way to any safeguarding concerns.

The three critical criteria are:

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

Procedures

Our procedure is based on the GDPR principles as listed above and the seven golden rules for sharing information in the Information sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers. We also follow the guidance on information sharing from the Local Safeguarding Partners

1. *Remember that the General Data Protection Regulations 2018 and human rights law are not barriers to justified information sharing as per the Children Act 1989 but provide a framework to ensure that personal information about living individuals is shared appropriately.*

    - Our policy and procedures on the GDPR and Information Sharing provide guidance to appropriate sharing of information both within the setting, as well as with external agencies.

2. *Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their consent, unless it is unsafe or if I have a legal obligation to do so. A Privacy Notice is given to parents at the point of registration to explain this further.*

    In our setting we ensure parents:

- Receive a copy of our Privacy Notice and information about our GDPR and Information Sharing Policy when starting their child in the setting and that they sign our Registration Form to say that they understand the circumstances in which information may be shared without their consent. This will only be when it is a matter of safeguarding a child or vulnerable adult;
- have information about our Safeguarding Children and Child Protection Policy; and
- have information about the other circumstances when information will be shared with external agencies, for example, with regard to any special needs the child may have or transition to school.

3. *Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.*

- Our staff discuss concerns about a child routinely in supervision and any actions are recorded in the child's file and on the supervision form that is kept in a lockable file.
    - Our manager routinely seeks advice and support from their line manager about possible significant harm.
- Our Safeguarding Children and Child Protection Policy sets out the duty of all members of our staff to refer concerns to our manager as designated person, or Deputy, who will contact children's social care (IFD) for advice where they have doubts or are unsure.
- The manager will seek advice if they need to share information without consent to disclose.

4. *Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.*

- We base decisions to share information without consent on judgements about the facts of the case and whether there is a legal obligation.
- Our guidelines for consent are part of this procedure.
- Our manager is conversant with this and she is able to advise staff accordingly.

5. *Consider safety and well-being: Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.*

In our setting we:

- record concerns and discuss these with our designated person and/or designated officer from the management team for child protection matters;
- record decisions made and the reasons why information will be shared and to whom; and
- follow the procedures for reporting concerns and record keeping as set out in our Safeguarding Children and Child Protection Policy.

6. *Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.*

- Our Safeguarding Children and Child Protection Policy and Children's Records Policy set out how and where information should be recorded and what information should be shared with another agency when making a referral.

7. *Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.*

- Where information is shared, we record the reasons for doing so in the child's file; where it is decided that information is not to be shared that is recorded too.

Consent

When parents choose our setting for their child, they will share information about themselves and their families. This information is regarded as confidential. Parents have a right to be informed that we will seek their consent to share information in most cases, as well as the kinds of circumstances when we may not seek their consent or may override their refusal to give consent. We inform them as follows:

- 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 welcome pack
- Parents sign our Registration Form at registration to confirm that they understand this.
- We ask parents 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.
- We give parents copies of the forms they sign.
- We consider the following questions when we assess the need to share:
  - Is there a legitimate purpose to us sharing the information?
  - Does the information enable the person to be identified?
  - Is the information confidential?
  - If the information is confidential, do we have consent to share?
  - Is there a statutory duty or court order requiring us to share the information?
  - If consent is refused, or there are good reasons for us not to seek consent, is there sufficient public interest for us to share information?
  - If the decision is to share, are we sharing the right information in the right way?
  - Have we properly recorded our decision?
- Consent must be freely given and *informed* - that is the person giving consent needs to understand why information will be shared, what will be shared, who will see information, the purpose of sharing it and the implications for them of sharing that information as detailed in the Privacy Notice.
- Consent may be *explicit*, verbally but preferably in writing, or *implicit*, implied if the context is such that sharing information is an intrinsic part of our service or it has been explained and agreed at the outset.
- Consent can be withdrawn at any time.
- We explain our GDPR and Information Sharing Policy to parents.

Separated parents

- Consent to share need only be sought from one parent. Where parents are separated, this would normally be the parent with whom the child resides. Where there is a dispute, we will consider this carefully.
- Where the child is looked after, we may also need to consult the Local Authority, as 'corporate parent' before information is shared.

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

People, risks and responsibilities.

Policy scope.

This policy applies to:

- Maidenbower Pre-School Playgroup
- All staff and volunteers of Maidenbower Pre-School Playgroup
- All parents/carers and children, suppliers and other people working on behalf of Maidenbower Pre-School Playgroup

It applies to all data that the playgroup holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus, any other information relating to individuals

Data protection risks.

This policy helps to protect Maidenbower Pre-School Playgroup from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the playgroup uses data relating to them.
- **Reputational damage.** For instance, the playgroup could suffer if hackers successfully gain access to sensitive data.

Responsibilities.

Everyone who works for or with Maidenbower Pre-School Playgroup has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The playgroups chairperson is ultimately responsible for ensuring that Maidenbower Pre-School Playgroup meets its legal obligations.
- **The playgroups Data Protection Officer is Emma Herbe** who is responsible for:
    - Keeping the committee and manager updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered in this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Maidenbower Pre-School Playgroup holds about them (also called “subject access requests”).
    - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services, the playgroup is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary. Working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines.

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required, employees can request it from the manager.
- **Maidenbower Pre-School Playgroup will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.

- Personal data **should not be disclosed** to unauthorised people, either within the playgroup or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required it should be deleted and disposed of.
- Employees **should request help** from their manager or the data protection officer (Emma Herbe) if they are unsure about any aspects of data protection.

Google Analytics.

We use Google Analytics to help record what page you view when visiting our website. All the information gathered is anonymous so we do not know who you are but can see what pages you have visited and what pages you have left and for how long.

We use the anonymous data collected to see what part of our site are performing well, what pages people are looking at and leaving on and some very basic information on what device, browser and operating system you are using. This data is collected to help us improve your experience when visiting our website.

To find out more information you can see GOOGLE ANALYTICS or OPT OUT IF YOU WISH

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the committee or data controller Emma Herbe.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them,** like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service.**
- Servers containing personal data should be **sited in a secure location,** away from general office space.
- Data should be **backed up frequently.** Those backups should be tested regularly, in line with the playgroup's standard backup procedures.

- All servers and computers containing data should be protected by **approved security software and a firewall.**
- All areas of our website use **SSL encryption.**

Data use.

Personal data is of no value to Maidenbower Pre-School Playgroup unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal **data should not be shared informally**.
- Data must be **encrypted before being transferred electronically.** The data controller Emma Herbe can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area.**
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy.

The law requires Maidenbower Pre-School Playgroup to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Maidenbower Pre-School Playgroup should put into ensuring its accuracy.

It is the responsibility of **all** employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary.** Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming parent's details when they call.
- Maidenbower Pre-School Playgroup will make it **easy for data subjects to update the information** Maidenbower Pre-School Playgroup holds about them. For instance, via the playgroup website and Tapestry.
- Data should be **updated as inaccuracies are discovered.** For instance, if a parent can no longer be reached on their stored telephone number, it should be removed from the data base or updated as soon as possible.

Subject access requests.

All individuals who are the subject of personal data held by Maidenbower Pre-School Playgroup are entitled to:

- Ask **what information** the playgroup holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the playgroup is **meeting its data protection obligations.**

If an individual contacts the playgroup requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller Emma Herbe at admin@maidenbowerplaygroup.org.uk

Individuals will be charged £25 per subject access request. The data controller Emma Herbe will aim to provide the relevant data within 14 days.

The data controller Emma Herbe will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons.

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies and for child protection and safeguarding purposes without the consent of the data subject.

Under these circumstances, Maidenbower Pre-School Playgroup **will** disclose requested data. However, the data controller Emma Herbe will ensure the request is legitimate, seeking assistance from the committee and from the playgroup's legal advisers where necessary. (Peninsular, Lawcall, EYA).

Providing information.

Maidenbower Pre-School Playgroup aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the playgroup has a privacy statement, setting out how data relating to individuals is used by the playgroup.

This is given out in your child's Welcome Pack. A version of this statement is also available on the playgroup's website: www.maidenbowerplaygroup.org.uk and also on the playgroups notice board.

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

We keep this policy under regular review. You will be notified of any changes where appropriate.

Legal framework

- General Data Protection Regulations (GDPR) (2018)
- Human Rights Act (1998)

This policy was adopted by		*(name of provider)*
On		*(date)*
Date to be reviewed		*(date)*
Signed on behalf of the provider		
Name of signatory		
Role of signatory (e.g., chair, director or owner)		