St Paul's Childcare

Confidentiality and Data Protection Policy

Written in conjunction with NMS 5

St Paul's Childcare will follow this policy, review it annually and update it as required.

The Person in Charge (Leader) of St Paul's Childcare will ensure that every member of staff understands this policy.

St Paul's Childcare will ensure that parents and carers are aware of this policy. We will ensure this policy is available to all via:
*St Paul's Childcare website
*The entrance of the childcare setting
*St Paul's C/W Primary School website
The policy may be requested from Reception at St Paul's C/W Primary School

Policy last updated – September 2020

Next policy update due – September 2021

REVIEWED BY

Name	**Signature**	**Date**
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Contents

Confidentiality and Data Protection Policy

This policy is relevant to all employees, volunteers, students on placement or work experience and members to the St Paul's Playgroup committee. Breaching this policy could lead to disciplinary procedures and serious incidents could lead to dismissal in line with the St Paul's disciplinary procedures.

Aim

Everyone has rights regarding how their personal information is treated. St Paul's Playgroup recognises the need to treat this information in an appropriate and lawful manner.

St Paul's Playgroup collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the playgroup. This information is gathered in order to enable it to provide its services and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Playgroup complies with its statutory obligations.

The Playgroup has a duty to inform individuals including parents and pupils of the information that it holds. This information should summarise why it is held and should identify any other parties to whom this information may be shared with. The Playgroup will advise individuals through a Fair Processing notice in concise, transparent, plain language and will be free of charge.

The aim of the St Paul's Playgroup is to ensure that all information regarding employees, volunteers, students on work experience and members of the St Paul's Playgroup committee, parents/carers/guardians and children is kept securely and confidentially. No information will be shared or revealed to persons or agencies that are not authorised to receive the information.

The Rights of the Child

This policy aims to ensure that the St Paul's Playgroup respects Children's Rights as stated in the United Nations Convention on The Rights of The Child, specifically:

Article 3: All organisations concerned with children should work towards what is best for each child.

Article 14: Children have the right to think and believe what they to and practice their religion, as long as they are not stopping other people from enjoying their rights.

Article 16: Children have a right to privacy. The law should protect them from attacks against their way of life, their good name, their families and their homes.

General Data Protection Regulation

The purpose of the regulation is not to prevent personal data from being processed, but to ensure that it is done fairly and without affecting the rights of the individual. In order for this to happen the General Data Protection Regulation (GDPR) sets out six principles, which are as follows:

The GDPR establishes six enforceable principles that must be adhered to at all times in that information must be:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible for those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purpose for which it 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 necessary for purposes that which the personal data is processed.
6. Processed in a manner that ensures appropriate security of the personal data.

The St Paul's Playgroup is committed to ensuring that personal data is processed, collected, is relevant, accurate and kept in accordance with the principles of the GDPR.

Further to the GDPR, the registered person responsible for St Paul's Playgroup is responsible for ensuring that records are maintained as required by Regulation 30, Schedule 3 of the Child Minding and Day Care (Wales) Regulations 2010 (as amended) which state that:

'Records that must be kept and maintained on the premises while the children are being cared for:

- The name, address and telephone number of the following:
    - The registered person
    - The responsible individual, where applicable
    - Every other person, living, working or employed on the premises where childcare is provided
    - Any other person who will regularly be in unsupervised contact with the relevant children'.

Code of Practice

The St Paul's Playgroup ensures that all employees, volunteers, students on work experience and members of the St Paul's Playgroup committee are provided with and expected to be aware of, to understand and follow this policy by:

- Ensuring that this policy is presented to new members of staff, volunteers, students on work experience and members of the St Paul's Playgroup committee as part of the Playgroups induction procedures.
- Ensuring that any and all documents or data that has been collected or processed is stored appropriately and securely.
- Ensuring that an appropriate password is required to gain access to any digital equipment or online platform that has been used to store data that has been collected or processed.
- Ensuring that personal data is not left in any public place or space.
- Ensuring that only individuals who are authorised to access and or who require access to any stored data are able to do so.
- Taking every step that is reasonably practicable to ensure the security of personal data which is processed and or kept by the St Paul's Playgroup.
- Clearly identifying who is authorised to access specific documents and files. (E.g. staff/volunteers/managers/committee members) For example this could include documents relating to an official meeting such as a committee or management meeting where minutes are kept and any decisions recorded.
- Requesting appropriate permission from parents/carers/guardians in situations where an external body wishes to gain access to any data that has been collected or process by the Playgroup. This could include, for example, ESTYN or St Paul's Church in Wales Primary School requesting to see a child's progress record as part of the quality accreditation scheme.
- Ensuring that a private space or room is used when discussing any personal information with parents/carers/guardians relating to their child.
- Following the guidance relating to the storage of any personal or confidential information.
- Following E-Safety Policy guidance with regard to the storage of any personal or confidential data on any digital platform.

E-Safety and Social Networks

The St Paul's Playgroup will follow its GDPR Policy in ensuring that all data that is collected or processed is stored securely and in line with the guidelines issued by the Information Commissioners Office.

The St Paul's Playgroup will follow the E-Safety Policy guidelines to ensure that there is no breach of confidentiality and to ensure digital data protection at all times. It will clearly state who is responsible for updating the details which are shared on any social network pages that are part of the setting's work following the E-Safety Policy guidelines on the use of Social Networks. This may include for example, the use of Twitter to publicise the work of the Playgroup.

The St Paul's Playgroup will provide a copy of its E-Safety Policy as a part of its induction procedures and expects all employees, volunteers, students on placement or work experience and members of the Playgroup committee to follow its E-Safety Policy when using social networks in their personal lives.

Sharing Information

Only the Registered Person/Leader or his/her deputy has the right to share confidential information with other agencies (e.g. CSSIW, Estyn, Social Services, St Paul's Church in Wales Primary School). When information needs to be shared with St Paul's Church in Wales Primary School, the Playgroup will:

- Follow the Information Commissioner's Office guidance and guidelines on sharing information when sharing quantitative data (e.g. education progression data).
- Ask for authorisation from the parent/carer/guardian to share the above data.
    - Where appropriate, information may be collected from and shared, following the receipt of a valid application, with the following:
        - The individual themselves or a parent/carer/guardian on behalf of a child.
        - Employers: former employers, current employers and prospective employers.
        - Inland Revenue
        - Home Office
        - Department for Work and Pensions
        - Police
        - Social Services
        - CSSIW
        - The playgroup/nursery's Registered Person/Management Committee Chairperson / Manager.
        - Cardiff County Council acting as the Local Education Authority
        - Estyn
        - St Paul's Church in Wales Primary School
        - Welsh Government.

The St Paul's Playgroup will follow the Information Commissioner's Office guidance and guidelines about sharing information when dealing with any application of this nature.

The Setting's Duty as a Holder of Personal Information

Personal information about staff, work experience students, volunteers, committee/management team members, parents/carers/guardians or children should not be shared with anyone inside or outside of the playgroup if there is no obvious need for the setting to do this in order to fulfil its role.

Storage of information

St Paul's Playgroup will:

- Follow this Policy's guidelines regarding the secure storage of information or data.
- Follow its E-Safety Policy guidelines to ensure that digital information is kept securely.
- Ensure that all confidential forms containing information and or data are locked away in a secure place.
- Ensure that any information is not transferred from one place to another or left in a public place.
- Clearly state who (e.g. staff/ volunteers/ managers/committee members) has access to specific files and documents (e.g. in a formal committee such as a committee meeting or management meeting) which is recorded with the decision noted.
- Adhere to the guidance and guidelines laid out in this Policy regarding sharing information with other agencies.
- Ensure that only authorised staff who have the right to access the data, and who require access to the data, are able to access the data.

Rights regarding Data which is held on an individual

An individual has the right to access the information which is kept about them from time to time and within reason. Applications should be made in writing to the Registered Person/Committee Chairperson/Leader, who will respond to the application. St Paul's Playgroup will follow the Information Commissioner's Office's guidance and guidelines when dealing with any applications of this nature.

Information Retention Period

St Paul's Playgroup will follow the statutory rules and guidelines as required by The Information Commissioners Office regarding the period of time that information is retained for.

Disposal of Information

St Paul's Playgroup will use appropriate and secure measures to ensure the correct disposal of any confidential and personal information takes place at an appropriate time.

St Paul's Playgroup will:

- Destroy paper records by using an appropriate document shredder.
- Destroy Memory Sticks and CD-ROMs by hand when they are no longer needed (e.g. by cutting them into small pieces with scissors).
- Delete digital images from any storage drive, including any back-up drive as well as deleting them from any corporate system itself.

Breach of Confidentiality

St Paul's Playgroup will consider any case of breaching confidentially, such as disclosing any personal information, as a severe matter. Any such occurrence will be investigated fully with reference made to the Staffing Policy. Breaching this policy may lead to a disciplinary procedure and a serious incident could lead to dismissal in line with the St Paul's Playgroup's disciplinary procedure.

Associated Policies

- GDPR Policy
- E-Safety Policy
- Staffing & Disciplinary Procedures Policy

Contacts and Useful Information

- The following publications and websites provide additional useful information:
    - Information Commissioner's Office: 'Register (notify) under the Data Protection Act'
        - https://ico.org.uk/for-organisations/register/
    - Information Commissioner's Office: 'Data protection self-assessment toolkit
        - https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment-toolkit/
    - The Information Commissioner's Office. Guide to Data Protection'
        - https://ico.org.uk/for-organisations/guide-to-data-protection/
    - The Information Commissioner's Office. Data Sharing'
        - https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/
    - The Information Commissioner's Office. Principle 7 – Security'
        - https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

Signature: Date: Date of review: