P04 Confidentiality and Data Protection Policy

Updated September 2023

This policy should be read in conjunction with policy P13 Safeguarding Child Policy and PC05 Guidance for Safer Working Practices.

Legal requirement: GDPR

All information on children, families and staff is kept securely and treated in confidence. Information will only be shared if the parents/carers/co-workers give their permission or there appears to be a child protection issue. The details are easily accessible if any information is required for inspection by Ofsted.

We are registered with the Information Commissioner's Office Data Register. We comply with the GDPR and the statutory guidance for the EYFS and Ofsted.

Principles

Article 5 of the GDPR sets out six Privacy Principles which we adhere to:

- We must have a lawful reason for collecting the data and how we process it should be fair and transparent.
- We only collect data for a specified purpose and only use it for that purpose.
- We only collect the data that is necessary.
- Data must be accurate and be kept up to date.
- Data must not keep or longer than is necessary.
- Data must be kept safe.

The Data Protection Lead (DPL) is the Playleader and is aware what type of data is held about the children and parents, what it is used for, where it is stored, how long it is kept and if it is shared elsewhere. The Chair of Trustees is responsible for data relating to staff and trustees.

Parents can request the erasure of data but the EYFS and Ofsted retention requirements will override this.

Explicit consent to retain and process data is given by parents using a clear consent form on the child's registration forms which requires a tick box and signature.

Third Party Data Processors

Any third party data processors (for example payroll) must be GDPR compliant. We will not share personal information about children, parents or staff with third parties except for safeguarding reasons or necessary contractual or legal administrative reasons.

Data Breaches

If we become aware of a data breach we will notify the ICO within 72 hours if it could result in discrimination, reputation damage, financial loss or loss of confidentiality. The individual to whom the breach relates will be informed and an investigation will be carried out into the circumstances of the breach. We will follow the Data Breach Procedure as set out by PATA in appendix 1.

Parental Access to Data

Data subjects (i.e. people we hold data about) can request to see all of the information that we hold about them. This can be a verbal request as well as in writing. If Staff/Committee Members receive a data subject access request they should immediately let the DPL know.

They will then follow the procedures in the Data Subject Access Request Policy in appendix 2. The time limit for responding is 1 month from the initial request so it is important that it is passed on immediately.

Purpose of Data Held

The personal data processed by us is held for the following purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Provision of childcare
- Education

All parents can view a copy of our policies and procedures. Key policies are available on the website and the full folder is available to view in setting.

We maintain a record of parents' emergency contact details, the contact details of the child's GP and appropriate signed consent forms.

If a child is identified as a child in need (section 17 of the Children Act 1989) we will, with the parent's permission, give appropriate information to referring agencies.

We expect parents to inform us of any changes in the child's home circumstances, care arrangements or any other change which may affect the child's behaviour such as a new baby, parents' separation, divorce or any bereavement.

All information shared will be kept confidential and will not be disclosed without the parent(s) consent, except as required by law. For example, if there appears to be a child protection issue. Please see the Safeguarding (Child Protection) Policy.

Ofsted may request to see our records at any time.

Parents have the right to inspect all records about their child at any time.

All accidents are recorded in an accident book.

All significant incidents are recorded in an incident book and will be shared and discussed with parents so that together we can work to resolve any issues.

All written records are kept securely locked away.

Individual children's files, observations and learning journeys are kept in a locked cupboard in setting. The cupboard is kept locked during out of session hours. Parents can request to see their child's file at any time. If the file is requested to go home then it must be signed out. Learning journeys are made available to parents regularly.

Computer records

We keep records relating to individual children on the play leader's computer. Parent's permission for these records to be held are obtained on the consent form signed as the child starts playgroup.

The information will be securely stored to prevent viewing of the information by others with access to the computer, for example, in password-protected files.

Backup files will be stored on an external hard drive and at the discretion of the directors on secure, encrypted on-line backup facility.

Backup files will be updated regularly to alleviate the event of data being lost.

Digital cameras, camera phones and photographs

The use of camera phones is allowed in setting during sessions, in the presence of other staff members, to take photos of children to use in Learning Journeys and for our closed Facebook page. We only use photos of children without their faces showing for our open Facebook page and only with the consent of parents.

The playgroup phone does have a camera facility and will be made available within setting. Parents are advised that should they wish to take photographs of their child during events, such as sports day, or nativity, it should be at close up range, and not contain images of other children.

It is playgroup policy not to publish photographs on any social networking media site other than the playgroup's own closed group; parents are encouraged to adhere to this policy. Only current parents are authorised to join the closed facebook group.

When a child leaves the setting their parents are removed from the closed facebook group. This applies also to staff members and trustees when they leave.

We will print photographs from our closed Facebook page of the children whilst at playgroup. The purpose of these photographs will be to enhance children's understanding and learning, for use in the child's learning journey and for displays inside the setting. Parents give permission via signed consent forms for photographs to be used on the Playgroup Website.

Photographs of children are printed regularly and are deleted at the end of the year from the Facebook page. These photographs will be kept in the children's learning journey and used for display purposes. No other copies are kept.

Occasionally photos may be downloaded via a password protected memory stick and taken off site to prepare promotional materials such as leaflets or for use on the website. When this takes place, additional written permission will be sought. Once these photos are finished with they will be deleted from both the memory stick and computer used.

Emailing photographs is prohibited unless express permission has been sought in advance.

At no point should a camera phone be taken into a nappy changing area/or toilet area. Photographs of children will only be taken in open plan areas of the setting and in full view of other members of staff.

The camera phone is used to support child/practitioner observations and learning and staff are mindful to be aware as to whether the child does not object to having his/her photograph taken.

Parents' permission is sought to photograph their child when on the premises and during outings via the registration form completed upon registering your child.

Role of the trustees/staff

It is the trustees' responsibility to ensure all staff having access to the equipment are fully trained in its use.

The staff will communicate with parents/carers appropriately and seek any written permission required by them for safe use by their children. If a member of staff should leave our employment, Ridgeway Playgroup will ensure they no longer have access via password to the equipment and that current passwords will be changed.

When not in use all equipment is stored in the locked cupboard in the main hall. Any records kept by the Chair or Treasurer are kept on their personal computers at home and is password protected and safely stored.

This policy was agreed by Trustees and Staff of Ridgeway Playgroup September 2021
Review Date: September 2024