36. Data Collection and Information Sharing

Version number	Dates produced & approved	Reason for production & revision	Author	Locations	Proposed next review date
V1.0	Sept 2017	EYFS requirement, incorporates Privacy Notice	K Jones & J Miller	Dropbox.com Website	Sept 2018
V2.0	Apr 2018	Updated to be in line with GDPR[1]	K Coupe & K Jones	Dropbox.com Website	April 2019
V3.0	29 Apr 2019	Updated in line with Keeping Children Safe in Education 2018	K Coupe & E Roberts	Dropbox.com Website	Apr 2020
V4.0	15 Dec 2020	Review of policy – minor alterations	K Coupe	Dropbox.com Website	February 2022
V5.0	19 Apr 2021	Inclusion of reference to the Pre-school's Cookie Preferences and Privacy Policy	K Coupe	Dropbox.com Website	June 2023
V6.0	7 July 2022	Updated • in line with Keeping Children Safe in Education (Sept 2021) Annex C re leavers; • inclusion of "Associated Policies & Procedures" section as per EY Safeguarding Audit section 175/157 2022	K Coupe E Pearce J Powell	Dropbox.com Website	Sept 2024
V7.0	17 May 2023	Document reviewed. Amendments to Data security section and who has access to staff details.	K Coupe	Dropbox.com Website	May 2025
V8-0	15 June 2023	Document amended to take account of revised ICO information should an employee (past/present) make a Subject Access Request	K Coupe	Dropbox.com Website	June 2025
V9.0	20 July 2023	Document updated confirming Setting is on the ICO Data register	K Coupe	Dropbox.com Website	July 2025
V10.0	26 Feb 2024	Updated with regards to • Working Together to Safeguard Children 2023; • inclusion of "Legal Framework" section.	K Coupe	Dropbox.com Website	Feb 2026

[1] General Data Protection Regulations (May 2018) (GDPR)

Version number	Dates produced & approved	Reason for production & revision	Author	Locations	Proposed next review date
V11.0	14 March 2024	Updated with regards ICO advice on sharing information in an emergency re staff wellbeing	K Coupe	Dropbox.com Website	March 2026
V12.0	24 April 2024	Updated with new section about the Freedom of Information Act 2000	K Coupe	Dropbox.com Website Hard Copy	April 2026
V13.0	3 July 26	Updated & reviewed	J Dyer	Website	July 27

Statement of Intent
North Nibley Pre-school recognises the importance of respecting the privacy of children and their parents and carers, while ensuring that they access high quality Pre-school care and education.

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

North Nibley Pre-school are a controller of your and your child's personal data under applicable data protection laws, including the General Data Protection Regulations 2018 (GDPR) and the Data Protection Act 2018 (DPA). As a registered charity, we are the Data Controller for the personal data we collect from you. This means that we decide what information we need to keep and why, and how we process and store that information. Our Data Protection Lead (DPL) is the Management Committee Chairperson who delegates day to day matters to the Pre-school's Administrator.

North Nibley Pre-school pays an annual subscription to the Information Commissioner's Office (ICO) to be included in their Data Protection Register. The Pre-school's reference number in this respect is ZB564430. The setting support officer is the Data Protection Officer. A copy of the certificate is stored at Preschool in the filing cabinet.

Aim
The aim of this policy is to ensure that all parents and carers are aware of how we keep their information and the circumstances in which we would share their information. A copy of our Privacy Notice is contained within our Welcome Pack paperwork and available on our website[2]. We also have a privacy notice with regards to cookies preferences which is also available on our website.

We ensure that the data we hold is accurate, as up to date as possible and not excessive. We only collect data that we are required to in line with the Childcare Acts 2006 and 2016, and set out in the Early Years Foundation Stage (EYFS) framework, which is mandatory for all early years providers in England.

The principles of the GDPR[3] shall be applied to all data processed:

[2] www.northnibleypreschool.co.uk

[3] Article 5

- processed fairly, lawfully and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not for further processed in any manner that is incompatible with those original purposes;
- accurate and, where necessary, kept up to date; any inaccuracies are erased or rectified without delay;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- not kept longer than is necessary for those purposes[4];
- protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and

Information Types
We keep two kinds of records on children attending our setting:

Developmental records
These include observations of children in the setting, samples of their work, summary developmental reports, next steps, records of achievement and transition records.

Personal Records
These include registration and admission forms, signed consents and correspondence concerning the child or family, eg. administration of medicine form or accident reports; reports or minutes from meetings concerning the child from other agencies, an ongoing record of relevant contact with parents and observations by staff on any confidential matter involving the child, such as developmental concerns or child protection matters. Together with parent declaration forms with regards to the free funding for 3 and 4 year olds and eligibility for the extended funding entitlement.

Method: Data Protection
Developmental Records
Each child has an individual record which is kept securely on Tapestry – an online learning journal. Parents are required to sign a consent form for information to be kept on Tapestry, before a child's Tapestry record is commenced. If a parent declines consent then their child's learning journey will be collated and maintained manually (ie. in paper format).

The online file can be accessed and contributed to by staff, and the child's parents and any other carer or relative that has been authorised access by both the child's parents and the Pre-school.

If a paper version is being used then this can be accessed at any time by the child's parents or whoever has parental responsibility, through request via their child's Key Person or the Playleader.

Personal Records
These files are only available to relevant staff and are kept securely under lock and key.

Our registration and admission forms require parents to give consent for us to hold and process their and their child's data.

[4] See Policy 35: Record Keeping

Historical files are retained for the statutory duration according to the GDPR and are kept in a secure location with restricted access.

Staff will not discuss personal information given by parents with other members of staff, except where it affects planning for the child's needs.

Staff induction includes an awareness of the importance of confidentiality in the role of the Key Person.

Method: Information Sharing

Children and/or their family

There are times when we are required to share information about a child or their family. Though the decision will never be made by an individual, but with the back-up of the Pre-school's management Committee. These three critical criteria are:

- There are concerns and there is *evidence* that the child may be suffering, or is at risk of suffering, significant harm.
- Where there is *reasonable cause to believe* that a child may be suffering, or at risk of suffering, significant harm.
- To prevent significant harm arising to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime (eg. domestic violence or other matters concerning the welfare of parents).

No single Early Years member of staff can have a full picture of a child's needs and circumstances so effective sharing of information between staff, local organisations and agencies is essential for early identification of need, assessment, and service provision to keep children safe.

Early Years staff aim to be as transparent as possible by telling families what information they are sharing and with whom, provided that it is safe to do so.

Where we have concerns as above, we would normally gain consent from families to share. If As good practice we always ask for written consent as a result of discussing a concern that we need to refer to a social care agency. This consent is kept in the child's file.

We do not seek consent from parents to share information[5] where we believe that a child, or sometimes a vulnerable adult, may be endangered by seeking to gain consent. For example, where we believe that a parent may try to cover up abuse, or threaten a child. Where evidence to support our concerns is not clear we may seek advice from Gloucestershire Early Years Team.

We only share relevant information that is accurate, factual, non-judgemental and up to date.

The decision to share information will always be made with the agreement and consent of 2 Pre-school Committee members.

[5] See Flowchart of when and how to share information at the end of Policy 4 Safeguarding Children and Child Protection

The GDPR and DPA do not prevent, or limit the sharing of information for the purposes of keeping children safe. Fears about sharing information **must not** be allowed to stand in the way of the need to promote welfare and protect the safety of children.

Where a child leaves the Pre-school, the Designated Safeguarding Lead (DSL) should ensure their child protection file is transferred to the new setting/school as soon as possible[6]. This file will be transferred separately from the child's main file, and the DSL will ensure secure transit and obtain a confirmation of receipt.

Employees
Data protection laws allow organisations to share personal information in an urgent or emergency situation, including to help prevent loss of life or serious physical, emotional or mental harm.

The ICO guidance[7] defines a mental health emergency as a situation in which the employer believes that someone is at risk or serious harm to themselves, or others, because of their mental health. This can include potential loss of life.

The ICO confirms that the employer will not get in trouble for sharing necessary and proportionate information with relevant and appropriate emergency services or health professionals that can help mitigate the risk of serious harm to the employee or to others. In addition, they advise that the employer could also share necessary and proportionate information with an employee's next of kin or emergency contact.

North Nibley Pre-school will ensure that all staff keep the details of their next of kin and emergency/mental health emergency contacts that we have on file up to date through regular review.

Suppliers
We annually check that our suppliers are compliant with GDPR. Copies of their Privacy Notice is kept for reference in a secure cabinet at the Pre-school.

Other Pre-School Records
All staff personnel files are kept in a secure location and are only accessible by the relevant line manager, ie. the Committee Chairperson, Setting Support Officer or the Play Leader. All staff have a copy of our Staff Privacy Notice. It is included in their induction pack.

Issues to do with the employment of staff, whether paid or unpaid, remain confidential to the people directly involved in making personnel decisions.

Students, when they are observing in the setting, are advised of our confidentiality policy and are required to respect it. Students need to obtain written consent from the parents of any children they wish to observe in the setting.

All the undertakings above are subject to the paramount commitment of North Nibley Pre-school, which is to the safety and well-being of the children who attend the pre-school.

Data Access Requests (Subject Access Requests (SARs))

[6] Within 5 days for an in-year transfer or within the first 5 days of the start of a new term.

[7] "Information sharing in mental health emergencies at work"

All individuals whose data is held by us, have a legal right to request access to such data or supplementary information held. The right of access allows individuals to be aware of and to verify the lawfulness of the processing.

Parents
Parents can have access to all written information about their child (except where data protection laws stipulate it is against the best interests of the child to do so) if a written request from the parent is received by the Management Committee Chairperson. The Pre-school will respond to the request within 30 days from the initial date of the request even if this was via telephone or in person. We will provide the information free of charge and in paper format. However, we reserve the right to charge a 'reasonable fee'[8] when a request is manifestly unfounded or excessive, particularly if it is repetitive. Please see Policy 41 'Data Subject Access Requests' which details how we deal with a request and your rights.

Parents do not have access to information about any other child than their own.

Employees
Employees, past and present, can submit a SAR, with respect to their personnel file. A data request must be made in writing to the relevant line manager. The Pre-school will respond within 30 days from the initial date of the request even if this was via telephone or in person. The setting will review the request and may ask for further clarification if a "general request" to see a file which contains a large amount of information, for example if the employee has been with the setting quite a few years. In this respect the time limit is paused until clarification received.

Personal information can cover more than one person, for example a witness statement used for internal disciplinary or investigatory issues or a whistleblowing report (this list is not exhaustive). Therefore, responding to a SAR may involve providing information that is about both the requester and someone else. The DPA 2018 states that the setting does not have to comply with a SAR if doing so means disclosing information which identifies someone else, except where:
- they consent to the disclosure; or
- it is reasonable to comply with the request without that person's consent.

To determine the latter, we will consider all the relevant circumstances, including:
- the type of information that we would disclose;
- any duty of confidentiality we owe to the other person/people;
- any steps we took to try to get the other person's consent;
- whether the other person is capable of giving consent; and
- any stated refusal of consent by the other person.

and we will refer to the ICO website to ensure that we are following their guidance "SARs: Q&A for employers".

[8] Based on administrative costs for providing the information

It should be noted that confidential references that we either provide to other organisations or that we receive at the start of an employee's employment are exempt from SAR requests – as per UK GDPR.

If the employee is unhappy with the SAR response received from North Nibley Pre-school, the employee should raise their concern, in the first instance, with the setting. We will take the complaint seriously and work with the requester to try and resolve it. However, if no resolution is found, the employee then has the right to raise a concern with the ICO.

Freedom of Information Act 2000 (FOIA)
The FOIA enables individuals and organisations to access information from public authorities. Charities are not "public authorities" and so are not directly subject to FOIA's requirements[9]. If a genuine FOIA request is received, rather than a GDPR Subject Access Request (SAR), the enquirer will be informed that North Nibley Pre-school is not obliged to provide the information. If known, we will direct the enquirer to any publicly available sources or a public authority that may have access to it. However, North Nibley Pre-school would be required to comply with any requests for personal data under the data protection legislation.

Fair Processing/Privacy Notice
North Nibley Pre-school shall be transparent about the intended processing of data and communicate these intentions via notifications to staff and parents prior to the processing of an individual's data.

Our Privacy Notice has been written in accordance with the Information Commissioner's Office (ICO) guidance and, due to the young age of the children attending our setting, has been written in a form understandable to parents and carers (see www.northnibleypreschool.co.uk). All parents whose children attend our setting receive a copy of our Privacy Notice and it is also displayed on our notice board at the setting. A separate Privacy Notice has been written for staff and all staff have received a copy.

The intention to share data relating to individuals to an organisation outside of our Pre-school shall be clearly defined within notifications (verbal and/or written) and details of the basis for the sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Data Security
Under the GDPR, North Nibley Pre-school has responsibilities to protect the personal information that we and our staff collect and use. This includes a requirement to have appropriate security to prevent it being accidentally or deliberately compromised. As such, physical data is stored in a locked filing cabinet, in a locked cupboard within the locked Village Hall. All IT devices (eg. laptops, ipads etc) used at the setting or by the Treasurer, Finance Administrator, Administrator and Setting Support Officer, are password protected and have up to date IT protection software installed. Data on these devices is backed up at least monthly if not more frequently. All IT devices are kept under lock and key. The Pre-school has a

[9] Part IV Schedule 1 of the legislations includes maintained schools and nursery schools, not Charity pre-schools, thus section 43 re "public authorities" does not apply.

Business Continuity Plan (BCP) with recovery solutions in place should North Nibley Village Hall become unavailable/inaccessible. The BCP is reviewed annually.

Only authorised people can access, alter, disclose or destroy personal data – as directed by the Management Committee Chairperson.

In order to assure the protection of all data being processed and inform decisions on processing activities, this policy will be reviewed annually, and before this time should any matters arise that need to be addressed.

Parents, carers and staff are required to report suspected data breaches[10] without delay to the Pre-school's DPL. Please refer to No 42 'Data Breach Procedure' for details on how we will deal with a reported breach.

Photographs and videos
Images of staff and children may be captured at appropriate times and as part of learning and development activities for use in the Pre-school only.

Unless prior consent from parents/carers/staff has been given, the Pre-school shall not utilise such images for publication or communication to external sources.

It is the Pre-school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.[11]

Archiving/Data disposal
North Nibley Pre-school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. To ensure that personal data is kept for no longer than necessary, North Nibley Pre-school will adhere to the requirements of its Record Keeping Policy[12]. This policy is reviewed every 2 years as a minimum.

All data held in paper format will be disposed of by shredding, using a cross-cut shredder, and in line with our Records Keeping policy. Photographs and videos downloaded to computers will be deleted within three months, and all photographs and videos will be deleted at the end of each Pre-school year. Electronic data held on laptops, ipads (or similar) or on a cloud provider, will be reviewed annually and data will be deleted according to our records keeping policy.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf. We will ensure that we use an IT asset disposal company which holds the required qualifications when the time comes. The company(ies) used must be accredited with ADSIA with distinction, Blancco or ISO 27001 etc.

[10] A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorised to do so.
[11] See No 21: Information and Communication Technology (ICT)
[12] No 35 Record Keeping

Legal framework

- General Data Protection Regulation 2018
- Data Protection Act 2019
- Human Rights Act 1998

Further guidance

- General Data Protection Regulation 2018 and Data Protection Act 2018
- Human Rights Act (1998)
- Keeping Children Safe in Education (latest version)
- Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (March 2015) – HM Government
- IT asset disposal for organisations.pdf (ICO)
- Working Together to Safeguard Children (latest version)
- ICO website: Information Commissioner's Office

Associate policies and procedures

- No 4: Safeguarding Children and Child Protection
- No 7: Confidentiality
- No 18 : Employment and staffing
- No 21: Information and Communication Technology (ICT)
- No 22 : Whistle Blowing procedure
- No 35: Record Keeping
- No 41: Data Subject Access Requests
- No 42: Data Breach Procedure