RECORD KEEPING POLICIES 2025-26

October 2025

Contents

Important Organisations Contact Details

Information Commissioner Office (ICO)
Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Website: https://ico.org.uk/

Local Safeguarding Procedures (LSP)
Hampshire Safeguarding Children Partnership (HSCP)
Email: hscp@hants.gov.uk Tel: 01962 876355

1. Record keeping policy

EYA Policy Template Reference: 07

Aim

We have record keeping systems in place for the safe and efficient management of the provision and to meet the needs of the children; that meet legal requirements for the storing and sharing of information within the framework of the GDPR and the Human Rights Act.

Objectives

- Children's records are kept on our online database, Famly, in personal files, divided into appropriate sections, and stored separately from their developmental records, or are kept electronically on management software systems.
- Children's personal files contain registration information as specified in procedure **Children's records and data protection**.
- The "Notes" section of each child's Famly profile is used to store other material described as confidential as required, such as Common Assessment Framework assessments, Early Support information or Education, Health and Care Plan (EHCP, case notes including recording of concerns, discussions with parents/carers, and action taken, copies of correspondence and reports from other agencies.
- Ethnicity data is only recorded where parents/carers have identified the ethnicity of their child themselves.
- Confidentiality is maintained by secure storage of files in a locked cabinet with access restricted to those who need to know. Client access to records is provided for within procedure **Client access to records**.
- Staff know how and when to share information effectively if they believe a family may require a particular service to achieve positive outcomes
- Staff know how to share information if they believe a child is in need or at risk of suffering harm.
- Staff record when and to whom information has been shared, why information was shared and whether consent was given. Where consent has not been given and staff have taken the decision, in line with guidelines, to override the refusal for consent, the decision to do so is recorded.

- Guidance and training for staff specifically covers the sharing of information between professions, organisations, and agencies as well as within them, and arrangements for training takes account of the value of multi-agency as well as single agency working.

Records

The following information and documentation are also held:

- name, address and contact details of the provider and all staff employed on the premises
- name address and contact details of any other person who will regularly be in unsupervised contact with children
- a daily record of all children looked after on the premises, their hours of attendance and their named key person
- certificate of registration displayed and shown to parents on request (displayed in the lobby)
- records of risk assessments
- record of complaints

Legal references

General Data Protection Regulation 2018

Freedom of Information Act 2000

Human Rights Act 1998

Statutory Framework for the Early Years Foundation Stage (DfE 2025)

Data Protection Act 2018

Further guidance

Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (HMG 2018 updated May 2024)

Business management mini-guide (Alliance publication)

2. Children's records and data protection

EYA Policy Template Reference: 07.1

During an outbreak of serious illness of disease there may be the need to keep additional records as part of outbreak management. A record is kept of individual cases of children/families who are self-isolating due to symptoms as per usual record-keeping procedures. In all cases the principles of data protection are maintained at Longparish Little School.

Principles of data protection: lawful processing of data

Personal data shall be:

a) *processed lawfully, fairly and in a transparent manner in relation to the data subject*

b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is not compatible for these purposes*

c) *adequate, relevant and necessary in relation to the purposes for which they are processed*

d) *accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay*

e) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*

f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")* Article 5 of the General Data Protection Regulations (2018)

Educators should process data, record and share information in line with the principles above.

General safeguarding recording principles

- It is vital that all relevant interactions linked to safeguarding children's and individual's welfare are accurately recorded.
- All recordings should be made as soon as possible after the event.
- Recording should be to a good standard and clear enough to enable someone other than the person who wrote it, to fully understand what is being described.

- Recording can potentially be viewed by a parent/carer, Ofsted inspector, by the successors of the educators who record, and may be used in a Family Court as relevant evidence to decide whether a child should remain with their biological parents or be removed to live somewhere else. Recording needs to be fair and accurate, non-judgemental in tone, descriptive, relevant, and should clearly show what action has been taken to safeguard a child and reflect decision-making relating to safeguarding.
- Recording should be complete, it should show what the outcome has been, what happened to referrals, why decisions were made to share or not share information, and it should contain summaries and minutes of relevant multi-agency meetings and multi-agency communication.
- If injuries or other safeguarding concerns are being described the description must be clear and accurate and should give specific details of the injury observed and where it is located.

The principles of GDPR and effective safeguarding recording practice are upheld at Longparish Little School

- Recording is factual and non-judgemental.
- The procedure for retaining and archiving personal data and the retention schedule and subsequent destruction of data is adhered to.
- Parents/carers and children where appropriate are made aware of what will be recorded and in what circumstances information is shared, prior to their child starting at the setting. Parents/carers are issued with the **Privacy Notice** and should give signed, informed consent to recording and information sharing prior to their child attending the setting. If a parent/carer would not expect their information to be shared in any given situation, normally, they should be asked for consent prior to sharing.
- There are circumstances where information is shared without consent to safeguard children. These are detailed below, but in summary, information can be shared without consent if an educator is unable to gain consent, cannot be expected to gain consent, or gaining consent places a child at risk.
- Records can be accessed by, and information may be shared with local authority professionals. If there are significant safeguarding or welfare concerns, information may also be shared with a family proceedings Court or the police. Educators are aware of information sharing processes and all families should give informed consent to the way the setting will use, store, and share information.

- Recording should be completed as soon as possible and within 5 working days as a maximum for safeguarding recording timescales.
- If a child attends more than one setting, a two-way flow of information is established between the parents/carers, and other providers. Where appropriate, comments from others (as above) are incorporated into the child's records.

Children's personal files

- Longparish Little School uses the online setting database, Famly, to store children's records.
- Access to children's personal files is restricted to those authorised to see them and make entries in them, this being the setting manager, deputy or designated person for child protection, the child's key person, or other staff as authorised by the setting manager.
- Children's files may be handed to Ofsted, as part of an inspection or investigation; they may also be handed to local authority staff conducting a S11 audit if authorisation is seen.

3. Privacy Notice

EYA Policy Template Reference: 07.1a

Longparish Little School's Privacy Notice

Longparish Little School
Longparish
Andover
Hampshire SP11 6PB

Introduction

Personal data is protected in accordance with data protection laws and used in line with your expectations. This privacy notice explains what personal data we collect, why we collect it, how we use it, the control you have over your personal data and the procedures we have in place to protect it.

When we refer to "we", "us" or "our", we mean Longparish Little School.

What personal data we collect at Longparish Little School

We collect personal data about you and your child to provide care and learning tailored to meet your child's individual needs. Personal details that we obtain from you include your child's: name, date of birth, address, and health, development and any special educational needs information. We will also ask for information about who has parental responsibility for your child and any court orders pertaining to your child.

Personal data that we collect about you includes: your name, home and work address, phone numbers, email address, emergency contact details, and family details.

We will only with your consent collect your national Insurance number or unique taxpayer reference (UTR) where necessary if you are self-employed and where you apply for up to 30 hours free childcare and early education. We also collect information regarding benefits and family credits. Please note that if this information is not provided, then we cannot claim funding for your child.

We also process financial information when you pay your childcare and early education fees by chip and pin or direct debit. We may collect other data from you when you voluntarily contact us.

Where applicable we will obtain details of your child's social worker, child protection plans from social care, and health care plans from health professionals and other health agencies.

We may collect this information in a variety of ways. For example, data will be collected from you directly in the registration form; from identity documents; from correspondence with you; or from health and other professionals.

Why we collect personal data and the legal basis for handling your data

We use personal data about you and your child to provide childcare and early education services and to fulfil the contractual arrangement you have entered. This includes using your data in the following ways:

- to support your child's wellbeing and development
- to effectively manage any special education, health or medical needs of your child whilst at the setting
- to carry out regular assessment of your child's progress and to identify any areas of concern
- to maintain relevant contact about your child's wellbeing and development
- to contact you in the case of an emergency
- to process your claim for free childcare and early education, if applicable

- to enable us to respond to any questions you ask
- to keep you updated about information which forms part of your contract with us
- to notify you of service changes or issues

With your consent, we would also like to:

- collect your child's ethnicity and religion data for monitoring purposes
- record your child's activities for their individual learning journal (this will often include photographs and videos of children during play)
- transfer your child's records to the receiving school when they transfer

If we wish to use any images of your child for training, publicity or marketing purposes we will seek your written consent. You are able to withdraw your consent at any time, for images being taken of your child and/or for the transfer of records to the receiving school, by confirming so in writing to the setting.

We have a legal obligation to process safeguarding related data about your child should we have concerns about their welfare.

Who we share your data with

As a registered early years provider to deliver childcare and early education services it is necessary for us to share data about you and/or your child with the following categories of recipients:

- Ofsted when there has been a complaint about the childcare and early education service or during an inspection
- banking services to process chip and pin and/or direct debit payments (not currently used)
- the local authority if you claim up to 30 hours free childcare
- the governments eligibility checker as above, if applicable
- our insurance underwriter, where applicable

We will also share your data:

- if we are legally required to do so, for example, by a law enforcement agency, court
- to enforce or apply the terms and conditions of your contract with us

- to protect your child and other children; for example, by sharing information with medical services, social services, or the police
- if it is necessary to protect our rights, property, or safety or to protect the rights, property, or safety of others
- with the school that your child will be attending, when they transfer, if applicable
- if we transfer the management of the provision out or take over any other organisation or part of it, in which case we may disclose your personal data to the prospective seller or buyer so that they may continue using it in the same way

Our nursery management and communication software provider may be able to access your personal data when carrying out maintenance task and software updates on our behalf. However, we have a written agreement in place which place this company under a duty of confidentiality.

We will never share your data with any organisation to use for their own purposes.

How do we protect your data?

We take the security of your personal data seriously. We have internal policies and strict controls in place to try to ensure that your data is not lost, accidentally destroyed, misused, or disclosed and to prevent unauthorised access.

Where we engage third parties to process personal data on our behalf, they are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Where do we store your data?

All data you provide to us is stored on secure computers or servers located within the UK or European Economic Area. We may also store paper records in locked filing cabinets.

Our third-party data processors will also store your data on secure servers which may be situated inside or outside the European Economic Area. They may also store data in paper files.

How long do we retain your data?

We retain your data in line with our retention policy a summary is below:

- You and your child’s data, including registers are retained 3 years after your child no longer uses the setting, or until our next Ofsted, after your child leaves our setting.

- Medication records and accident records are kept for longer according to legal requirements.
- Learning journeys are maintained by the setting and available at your request when your child leaves. Records are kept and archived in line with our data retention policy.
- In some cases (child protection or other support service referrals), we may need to keep your data longer, only if it is necessary to comply with legal requirements. We will only keep your data for as long as is necessary to fulfil the purposes it was collected for and in line with data protection laws.

Your rights with respect to your data

As a data subject, you have several rights. You can:

- request to access, amend or correct the personal data we hold about you and/or your child
- request that we delete or stop processing your and/or your child's personal data, for example where the data is no longer necessary for the purposes of processing or where you wish to withdraw consent
- request that we transfer your and your child's personal data to another person

If you wish to exercise any of these rights at any time please contact the manager at the setting by email, telephone or when you attend the setting.

How to ask questions about this notice

If you have any questions, comments, or concerns about any aspect of this notice or how we handle your data please contact the manager at the setting.

How to contact the Information Commissioner Office (ICO)

If the manager is not able to address your concern, please contact the Chair of Longparish Little School Management Committee chair@longparishlittleschool.org.uk

If you are concerned about the way your data is handled and remain dissatisfied after raising your concern, you have the right to complain to the Information Commissioner Office (ICO). The ICO can be contacted at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or https://ico.org.uk/.

Changes to this notice

We keep this notice under regular review. Any changes to this notice will be shared with you so that you may be aware of how we always use your data.

4. Privacy Notice - Staff

1. About this Privacy Notice

Under data protection law, you have a right to know about how Longparish Little School uses the personal data we hold. This privacy notice explains how we collect, store and use personal data about you. This Privacy Notice applies to all adults who are employed by Longparish Little School ("staff"). This includes those on permanent contracts; temporary contracts, cover staff and apprentices.
If you have any questions about data and privacy, please speak to the Data Officer for Longparish Little School: Claire Nash.

2. Why We Collect Personal Data: Our Legal and Contractual Framework

We are required by law to collect, hold and use (or 'process') data and information about you and your family whilst you are employed by Longparish Little School.
The Early Years Foundation Stage (EYFS) requires us to "have effective systems in place to ensure that practitioners, and any other person who is likely to have regular contact with children, are suitable". The EYFS also requires us to secure enhanced criminal records checks (DBS checks); and to record information about staff qualifications and identity checks. We are also required to disclose whether individuals may be subject to disqualification or whether action by their close family or household members may result in disqualification by association. We are also required to confirm that any medication taken by staff will not impair their ability to work with children. We must offer suitable training. We must ensure staff ratios are maintained.
OFSTED and the Charity Commission require us to maintain records to show that the leadership and management of Pre-School meets legal requirements. We are also required by financial legislation to keep accounting data including information about pay, pensions etc. and by health and safety legislation to keep records concerning, amongst other issues, accidents at work.
The EYFS requires that all the data is held securely and only accessible to those who have a right or a professional need to see.

3. The Personal Data We Hold

The data we collect, use, store and share (where appropriate) may include, but is not restricted to:

• Your name, address, telephone numbers, date of birth, gender, qualifications and work history and copies of documents confirming these details.
• Your national insurance number; bank details and information about your pay, taxation, pensions and benefits as appropriate.
• Information confirming background checks including enhanced criminal records checks (DBS); and references (as appropriate)
• Information about your health, medication and medical conditions. This may include reports from other professionals which are held on file by us. This may include any information you give us about dietary needs/allergies.
• Accident records, including those required by the Control of Substances Hazardous to Health (COSHH) regulations.
• Records of your attendance and absences.
• Any information recording any safeguarding concerns; Whistleblowing or Complaints.
• Copies of job application forms including Curriculum Vitae and other supporting documents. Records of interviews and assessments.
• Records of staff supervisions, appraisals or other work-related personnel meetings. Information relating to any disciplinary and/or grievance procedures.
• Information about training undertaken whilst employed by Longparish Little School.
• You may have either completed, or contributed to, records of general staff meetings, INSET days, planning meetings etc. and have been recorded as undertaking actions from our Improvement Plan or outcomes from audits or inspections.
• You may appear in, or have recorded, written outcomes or discussions with other agencies or professionals (for example, SEND reviews and EHCP meetings; safeguarding reviews etc.).
• Your picture may appear on the Pre-School website; newsletters or other information/publicity documents.

4. How We Use Your Data

We use your personal data to, for example:
• Confirm that our recruitment procedures meet the requirements of “Safer Recruitment”
• Confirm that you are suitable for your role at Pre-School on recruitment and ongoing throughout your employment contract
• Enable you to be paid; and for the correct pension contributions and entitlements, taxation and benefits to be applied as appropriate
• Support effective performance management, training and development

• Ensure that the Pre-School is run in accordance with the law and our regulatory framework; and
• Ensure that the contract of employment between yourself and the Pre-School is fulfilled
The majority of the information we collect and hold on you is mandatory in order to fulfil or evidence our legal and regulatory requirements. We will make it clear when we collect personal information that is optional, and you have the right to withdraw or withhold this consent at any time.

5. How We Store Data

Maintaining your privacy and the confidentiality of your data and information is important. Most of the data we receive from you or about you is held on paper in your individual staff file. Staff files are held securely in lockable filing cabinets in the office or on Famly, our password protected online preschool management tool. Famly stores data in an industry standard AES-256 encrypted database. The data is synched securely between multiple zones in Frankfurt for high durability and availability. The database is also backed up fully once a day, every day and by-the-second incremental backup. Payroll and pension data is retained electronically by our Administrator, Sally Lawman, and is password protected.

6. How Long We Keep Records

Our Data Retention Document sets out the retainment periods for the data we collect. We will not store or keep personal data for longer than is necessary or required by law. When we destroy records, we shred paper records; and any electronic files are deleted.

7. Data Sharing

The law requires us to share some personal information. This includes sharing data with:
• statutory authorities if there is a safeguarding concern
• the Local Authority and the Department of Education
• OFSTED, when we renew or update our registration and when they come to inspect us.
• the Charity Commission, in order to maintain our registration as a charity
• other regulatory authorities that may need access to our records, for example, financial auditors or health and safety inspectors or organisations.
We share the personal information you provide when you complete your DBS check form with the government's Disclosure and Barring Service. This is managed online by Capita Recruitment and Vetting Service.

Your bank, salary and other pay details is shared with the Administrator. Personal data will also be shared with Her Majesty's Revenue and Customs (HMRC) in order to facilitate taxation.
If you have a pension, we will share some details with the pension processor in order to administer your pension.
Some of your personal details may be shared with the Parent Committee: The Chair, Secretary, Treasurer and/or other members if nominated by the Chair and as appropriate. The purpose of sharing information with the Committee is generally, but not limited to, supporting the assessment of pay and pay rises; and performance management.
We will not share your data with any other third parties without your permission unless the law requires us to do so. We will never sell your data to third parties for marketing purposes; or use your data to make automated decisions.

8. Your rights

You have the right to:
• Ask to see, amend or update your personal data
• In certain circumstances, ask that we delete, destroy or stop processing your personal data
• Ask that we transfer your personal data to another person
If you wish to exercise any of these rights, please speak to the Pre-School Leader or the Administrator.
You may be asked to put your request in writing.

9. Complaints and Contact Details

In the majority of cases, we would expect to be able to respond to any questions or comments about how we collect and use your personal data sufficient to satisfy any concerns you may have. However, if you remain dissatisfied you may:
• Make a formal Complaint to Pre-School, following our Complaints Procedure. (Details are in the
Parent Handbook and in our Complaints Policy, which is published on our website.)
• Make a complaint to the Information Commissioner's Office (ICO). You can contact the ICO online,
(www.ico.org.uk); or by phone (030 123 1113). You can also write to them at: ICO, Wycliffe House,
Water Lane, Wilmslow, Cheshire, SK9 5AF.

10. Review

This Privacy Notice will be subject to regular reviews in line with ICO guidance.

5. Privacy Notice – Trustees & Committee members

This statement explains how Longparish Little School handles and uses personal data that we collect about trustees and committee members.

1. Longparish Little School holds and processes information about you to enable us to fulfil our governance responsibilities as a charity and charitable company. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the Charity and manage our relationship with you lawfully and appropriately whilst you are working for us. This includes using information to enable us to comply with any legal requirements, pursue the legitimate interests of the Charity and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

2. Much of the information we hold will have been provided by you, but some may come from other sources such as referees.

3. The sort of information we hold includes your name, contact details, date of birth, correspondence with or about you; details of other trustee and company involvement.

4. You may also be referred to in company documents and records in the course of carrying out your duties and the business of the company. This will include meetings attended and contributions made at meetings, as recorded in minutes. Minutes are retained for 10 years.

5. Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

6. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to pension or health insurance schemes.

8. Your personal data will be retained only as long as is necessary for the purpose for which it was collected, and in accordance with our Data Protection Policy. Data will be securely destroyed when no longer required.

Your rights

10. Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

11. If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

12. You have the right to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the GDPR or DPA 18 with regard to your personal data.

Identity and contact details of controller and data protection officer

13. Longparish Little School is the controller and processor of data for the purposes of the DPA 2018 and GDPR.

14. If you have any concerns as to how your data is processed you can contact:

admin@longparishlittleschool.org.uk

6. Privacy Notice – Job Applicants

Introduction

At Longparish Little School we take your privacy seriously and are committed to ensuring that your personal data is protected in accordance with data protection laws and used in line with your expectations.

This privacy notice explains what personal data we collect, why we collect it, how we use it, the control you have over your personal data and the procedures we have in place to protect it.

When we refer to "we", "us" or "our", we mean Longparish Little School.

Our full legal information as a data controller, is:

Longparish Little School a charity registered in England Wales (number 1001065) with its registered address at Longparish, Andover, Hampshire SP11 6PB.

What personal data we collect

As part of any recruitment process, we collect and process personal data relating to job applicants. This means that we need to collect a range of information about you. This includes:

your name, address and contact details, including email address and telephone number.

details of your qualifications, training, skills, experience and employment history;

information about your current level of remuneration;

whether or not you have a disability for which we need to make reasonable adjustments during the recruitment process;

information about your entitlement to work in the UK; and

your membership of any professional bodies.

If you are given a conditional offer of employment, you will be required to provide the following additional personal information:

bank details, NI number and P45, to process salary payments;

emergency contact details, so we know who to contact in case you have an emergency at work;

details of your medical history, to check your fitness for the role; and

whether if appointed, there is a potential conflict in interest (our code of conduct requires all staff to declare this).

We collect this information in a variety of ways. For example, data might be contained in application forms/CVs, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including tests.

We may also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. We will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so.

Why we collect personal data and the legal basis for handling your data

We need to process data at your request prior and in order to enter into an employment contract with you.

In some cases, we need to process data to comply with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to any legal claims.

With your consent we may process special categories of data, such as information about ethnic origin, marital status, or religion or belief, to monitor recruitment statistics.

We may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. We process such information to carry out our legal obligations and exercise specific rights in relation to employment.

We are legally required to obtain enhanced Disclosure and Barring Service (DBS) checks about criminal convictions and offences, and check your suitability in line with the Disqualifications by Association Regulations. Where we seek this information, we do so because it is necessary for us to carry out our legal obligations and exercise specific rights in relation to employment. For certain child care roles, we are legally obligated to consider the medical history of job applicants. In other cases, it is in our legitimate interest to do so.

If your application is unsuccessful, in some circumstances, we may wish to keep your personal data on file in case there are future employment opportunities for which you may be

suited. We will ask for your consent before we keep your data for this purpose and you are free to withdraw your consent at any time.

Who we share your data with

We will not share your data with third parties, unless your application for employment is successful and we make you an offer of employment. We will then share your data with:

current/former employers to obtain references for you;

our DBS processor and the DBS to obtain necessary criminal records checks (only if applicable); and

the Pensions Regulator, our pensions provider (NEST) if you choose or are automatically enrolled into our occupational pension scheme.

Our online email host may be able to access your personal data when carrying out maintenance task and software updates. However, we have a written agreement in place which place this company under a duty of confidentiality.

For some roles, we have a legal obligation to share your personal information with Ofsted, prior to you being able to commence employment with us.

How do we protect your data?

We take the security of your personal data seriously. We have internal policies and strict controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed and to prevent unauthorised access.

Where do we store your data?

All data you provide to us is stored on secure computers or servers located in the UK or the European Economic Area. We also store paper records in locked filing cabinets.

Our third party processors will also store your data on secure IT systems which may be situated inside or outside of the European Economic Area. They may also store data in paper files.

How long do we retain your data?

If your application for employment is unsuccessful, we will hold your data on file for six months after the end of the relevant recruitment process. If you agree to allow us to keep your personal data on file, we will hold your data on file for a further time period for consideration for future employment opportunities. We will ask for your consent to keep your data for this purpose. At the end of that period or once you withdraw your consent, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in our Employee Privacy Notice.

Your rights with respect to your data

As a data subject, you have a number of rights. You can:

request to access, amend or correct the personal data we hold about you;

request that we delete or stop processing your personal data, for example where the data is no longer necessary for the purposes of processing;

request that we transfer your personal data to another person; and

How to ask questions about this notice

If you have any questions, comments or concerns about any aspect of this notice or how we handle your data please contact Sally Lawman, Business Manager, via email admin@longparishlittleschool.org.uk

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to us during the recruitment process. However, if you do not provide the information, we may not be able to process your application.

How to contact the Information Commissioner Office (ICO)

If you are concerned about the way your data is handled and remain dissatisfied after raising your concern with our Manager, you have the right to complain to the Information Commissioner Office (ICO). The ICO can be contacted at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or https://ico.org.uk

7. Confidentiality, recording and sharing information

EYA Policy Template Reference: 07.2

Most things that happen between the family, the child and the setting are confidential to Longparish Little School setting. In certain circumstances information is shared, for example, a child protection concern will be shared with other professionals including social care or the police, and settings will give information to children's social workers who undertake S17 or S47 investigations. Normally parents/carers should give informed consent before information is shared, but in some instances, such as if this may place a child at risk, or a serious offence may have been committed, parental consent should not be sought before information is shared. Local Safeguarding Partners (LSP) procedures should be followed when making referrals, and advice sought if there is a lack of clarity about whether parental consent is needed before making a referral due to safeguarding concerns.

- Staff discuss children's general progress and well-being together in meetings, but more sensitive information is restricted to designated persons and key persons and shared with other staff on a need-to-know basis.

- Members of staff do not discuss children with staff who are not involved in the child's care, nor with other parents/carers or anyone else outside of the organisation, unless in a formal and lawful way.
- Discussions with other professionals should take place within a professional framework, not on an informal basis. Staff should expect that information shared with other professionals will be shared in some form with parent/carers and other professionals, unless there is a formalised agreement to the contrary, i.e. if a referral is made to children's social care, the identity of the referring agency and some of the details of the referral is likely to be shared with the parent/carer by children's social care.
- It is important that members of staff explain to parents that sometimes it is necessary to write things down in their child's file and explain the reasons why.
- When recording general information, staff should ensure that records are dated correctly, and the time is included where necessary and signed.
- Welfare/child protection concerns are recorded on a **Child Protection Expression of Concern form (Safeguarding Policies)**. Information is clear and unambiguous (fact, not opinion), although it may include the educator's thoughts on the impact on the child.
- Records are non-judgemental and do not reflect any biased or discriminatory attitude.
- Not everything needs to be recorded, but significant events, discussions and telephone conversations must be recorded at the time that they take place.
- Recording should be proportionate and necessary.
- When deciding what is relevant, the things that cause concern are recorded as well as action taken to deal with the concern. The appropriate recording format is filed within the child's file.
- Information shared with other agencies is done in line with these procedures.
- Where a decision is made to share information (or not), reasons are recorded.
- Staff may use a computer to type reports, or letters. Where this is the case, the typed document is deleted from the computer and a copy is retained on the child's Famly profile in the Notes section, marked confidential.
- Electronic copy is downloaded onto a memory stick, labelled with the child's name and stored in the child's file. No documents are kept on a hard drive because computers do not have facilities for confidential user folders.

- The setting is registered with the Information Commissioner's Office (ICO). Staff are expected to follow guidelines issued by the ICO, at https://ico.org.uk/for-organisations/guidance-index/
- Additional guidance in relation to information sharing about adults is given by the Social Care Institute for Excellence, at www.scie.org.uk/safeguarding/adults/practice/sharing-information
- Staff should follow guidance including Working Together to Safeguard Children (DfE 2023); Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers 2024 and What to do if you're Worried a Child is Being Abused (HMG 2015)

Confidentiality definition

- Personal information of a private or sensitive nature, which is not already lawfully in the public domain or readily available from another public source, and has been shared in a relationship, where the person giving the information could reasonably expect it would not be shared with others.
- Staff can be said to have a 'confidential relationship' with families. Some families share information about themselves readily; members of staff need to check whether parents/carers regard this information as confidential or not.
- Parents/carers sometimes share information about themselves with other parents/carers as well as staff; the setting cannot be held responsible if information is shared beyond those parents/carers whom the person has confided in.
- Information shared between parents/carers in a group is usually bound by a shared agreement that the information is confidential and not discussed outside. The setting manager is not responsible should that confidentiality be breached by participants.
- Where third parties share information about an individual; staff need to check if it is confidential, both in terms of the party sharing the information and of the person whom the information concerns.
- Information shared is confidential to the setting.
- Educators ensure that parents/carers understand that information given confidentially will be shared appropriately within the setting (for instance with a designated person, during supervision) and should not agree to withhold information from the designated person or their line manager.

Breach of confidentiality

- A breach of confidentiality occurs when confidential information is not authorised by the person who provided it, or to whom it relates, without lawful reason to share.
- The impact is that it may put the person in danger, cause embarrassment or pain.
- It is not a breach of confidentiality if information was provided on the basis that it would be shared with relevant people or organisations with lawful reason, such as to safeguard an individual at risk or in the public interest, or where there was consent to the sharing.
- Procedure **Children's records and data protection (Section 2)** must be followed.

Exception

- GDPR enables information to be shared lawfully within a legal framework. The Data Protection Act 2018 balances the right of the person about whom the data is stored with the possible need to share information about them.
- The Data Protection Act 2018 contains "safeguarding of children and individuals at risk" as a processing condition enabling "special category personal data" to be processed and to be shared. This allows educators to share without consent if it is not possible to gain consent, if consent cannot reasonably be gained, or if gaining consent would place a child at risk.
- Confidential information may be shared without authorisation - either from the person who provided it or to whom it relates, if it is in the public interest and it is not possible or reasonable to gain consent or if gaining consent would place a child or other person at risk. The Data Protection Act 2018 enables data to be shared to safeguard children and individuals at risk. Information may be shared to prevent a crime from being committed or to prevent harm to a child, Information can be shared without consent in the public interest if it is necessary to protect someone from harm, prevent or detect a crime, apprehend an offender, comply with a Court order or other legal obligation or in certain other circumstances where there is sufficient public interest.
- Sharing confidential information without consent is done only in circumstances where consideration is given to balancing the needs of the individual with the need to share information about them.
- When deciding if public interest should override a duty of confidence, consider the following:
    - is the intended disclosure appropriate to the relevant aim?

- what is the vulnerability of those at risk?
- is there another equally effective means of achieving the same aim?
- is sharing necessary to prevent/detect crime and uphold the rights and freedoms of others?
- is the disclosure necessary to protect other vulnerable people?

The decision to share information should not be made as an individual, but with the backing of the designated person who can provide support, and sometimes ensure protection, through appropriate structures and procedures.

Obtaining consent

Consent to share information is not always needed. However, it remains best practice to engage with people to try to get their agreement to share where it is appropriate and safe to do so.

Using consent as the lawful basis to store information is only valid if the person is fully informed and competent to give consent and they have given consent of their own free will, and without coercion from others, Individuals have the right to withdraw consent at any time.

You should not seek consent to disclose personal information in circumstances where:

- someone has been hurt and information needs to be shared quickly to help them
- obtaining consent would put someone at risk of increased harm
- obtaining consent would prejudice a criminal investigation or prevent a person being questioned or caught for a crime they may have committed
- the information must be disclosed regardless of whether consent is given, for example if a Court order or other legal obligation requires disclosure

NB. The serious crimes indicated are those that may harm a child or adult; reporting confidential information about crimes such as theft or benefit fraud are not in this remit.

- Settings are not obliged to report suspected benefit fraud or tax evasion committed by clients, however, they are obliged to tell the truth if asked by an investigator.
- Parents/carers who confide that they are working while claiming should be informed of this and should be encouraged to check their entitlements to benefits, as they it may be beneficial to them to declare earnings and not put themselves at risk of prosecution.

Consent

- Parents/carers share information about themselves and their families. They have a right to know that any information they share will be regarded as confidential as outlined in the **Privacy Notice (Section 3)**. They should also be informed about the circumstances, and reasons for the setting being under obligation to share information.
- Parents/carers are advised that their informed consent will be sought in most cases, as well as the circumstances when consent may not be sought, or their refusal to give consent overridden.
- Where there are concerns about whether to gain parental consent before sharing information, for example when making a Channel or Prevent referral the setting manager must inform their line manager for clarification before speaking to parents/carers.
- Consent must be 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.

Separated parents/carers

- Consent to share need only be sought from one parent/carer. Where parents/carers are separated, this would normally be the parent/carer with whom the child resides.
- Where there is a dispute, this needs to be considered carefully.
- Where the child is looked after, the local authority, as 'corporate parent' may also need to be consulted before information is shared.

Age for giving consent

- A child may have the capacity to understand why information is being shared and the implications. For most children under the age of eight years in a nursery or out of school childcare context, consent to share is sought from the parent/carer, or from a person who has parental responsibility.
- Young persons (16-19 years) are capable of informed consent. Some children from age 13 onwards may have capacity to consent in some situations. Where they are deemed not to have capacity, then someone with parental responsibility must consent. If the child is capable and gives consent, this may override the parent's/carer's wish not to give consent.
- Adults at risk due to safeguarding concerns must be deemed capable of giving or withholding consent to share information about them. In this case 'mental

capacity' is defined in terms of the Mental Capacity Act 2005 Code of Practice (Office of the Public Guardian 2007). It is rare that this will apply in the context of the setting.

Ways in which consent to share information can occur

- Policies and procedures set out the responsibility of the setting regarding gaining consent to share information, and when it may not be sought or overridden.
- Information in leaflets to parents/carers, or other leaflets about the provision, including privacy notices.
- Consent forms signed at registration (for example to apply sun cream).
- Notes on confidentiality included on every form the parent/carer signs.
- Parent/carer signatures on forms giving consent to share information about additional needs, or to pass on child development summaries to the next provider/school.

Further guidance

Working Together to Safeguard Children (DfE 2023)

Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (HMG 2024)

What to do if you're Worried a Child is Being Abused (HMG 2015)

Mental Capacity Act 2005 Code of Practice (Office of the Public Guardian 2007)

8. Client access to records

EYA Policy Template Reference: 07.3

Under the General Data Protection Regulations there are additional rights granted to data subjects which must be protected by Longparish Little School.

The parent/carer is the 'subject' of the file in the case where a child is too young to give 'informed consent' and has a right to see information that the setting has compiled on them.

- If a parent/carer wishes to see the file, a written request is made, which the setting acknowledges in writing, informing the parent/carer that an arrangement will be made for him/her to see the file contents, subject to third party consent.
- Information must be provided within 30 days of receipt of request. If the request for information is not clear, the manager must receive legal guidance, for instance, from Law-Call for members of the Alliance. In some instances, it may be necessary to allow

extra time in excess to the 30 days to respond to the request. An explanation must be given to the parent/carer where this is the case. The maximum extension time is 2 months.

- A fee may be charged to the parent/carer for additional requests for the same material, or any requests that will incur excessive administration costs.
- The setting manager informs their line manager/committee and legal advice is sought.
- The setting manager goes through the file and ensures all documents are filed correctly, entries are in date order and that there are no missing pages. They note any information, entry or correspondence or other document which mentions a third party. The setting manager should always ensure that recording is of good quality, accurate, fair, balanced and proportionate and should have quality assurance processes in place to ensure that files are checked for quality regularly and that any issues are addressed promptly.
- Each of those individuals are written to explaining that the subject of the file has requested sight of the file which contains a reference to them, stating what this is.
- They are asked to reply in writing to the setting manager giving or refusing consent for disclosure of that material.
- Copies of these letters and their replies are kept on the child's file.
- Agencies will normally refuse consent to share information, and the parent should be redirected to those agencies for a request to see their file held by that agency.
- Entries where you have contacted another agency may remain, for example, a request for permission from social care to leave in an entry where the parent was already party to that information.
- Each family member and/or carer noted on the file is a third party, so where there are separate entries pertaining to each parent/carer, stepparent, grandparent etc, each of those must be written to regarding third party consent.
- Members of staff should also be written to, but the setting reserves the right under the legislation to override a refusal for consent, or just delete the name and not the information.
    - If the member of staff has provided information that could be considered 'sensitive,' and the staff member may be in danger if that information is disclosed, then the refusal may be granted.

- If that information is the basis of a police investigation, then refusal should also be granted.
- If the information is not sensitive, then it is not in the setting's interest to withhold that information from a parent. It is a requirement of the job that if a member of staff has a concern about a child and this is recorded; the parents/carers are told this at the start and in most cases, concerns that have been recorded will have been discussed already, so there should be no surprises.
- The member of staff's name can be removed from an entry, but the parent/carer may recognise the writing or otherwise identify who had provided that information. In the interest of openness and transparency, the setting manager may consider overriding the refusal for consent.
- In each case this should be discussed with members of staff and decisions recorded.

- When the consent/refusals have been received, the setting manager takes a photocopy of the whole file. On the copy file the document not to be disclosed is removed (e.g. a case conference report) or notes pertaining to that individual in the contact pages blanked out using a thick marker pen.
- The copy file is then checked, and legal advisors verify that the file has been prepared appropriately, for instance, in certain circumstances redaction may be appropriate, for instance if a child may be damaged by their data being seen by their parent/carer, e.g. if they have disclosed abuse. This must be clarified with the legal adviser.
- The 'cleaned' copy is then photocopied again and collated for the parent to see.
- The setting manager informs the parent/carer that the file is now ready and invites him/her to make an appointment to view it.
- The setting manager and their line manager/trustee/committee member etc… meet with the parent/carer to go through the file, explaining the process as well as what the content records about the child and the work that has been done. Only the persons with parental responsibility can attend that meeting, or the parent's/carer's legal representative or interpreter.
- The parent/carer may take a copy of the prepared file, but it is never handed over without discussion.
- It is an offence to remove material that is controversial or to rewrite records to make them more acceptable. If recording procedures and guidelines have been followed, the

material should reflect an accurate and non-judgemental account of the work done with the family.

- If a parent/carer feels aggrieved about any entry in the file, or the resulting outcome, then the parent/carer should be referred to section **Complaints procedure for parents/carers and service users (Working in partnership with parents & other agencies Policy)**.
- The law requires that information held must be accurate, and if a parent/carer says the information held is inaccurate then the parent/carer has a right to request it to be changed. However, this only pertains to factual inaccuracies. Where the disputed entry is a matter of opinion, professional judgement, or represents a different view of the matter than that held by the parent/carer, the setting retains the right not to change the entry but can record the parent's/carer's view. In most cases, a parent/carer would have had the opportunity at the time to state their side of the matter, and this should have been recorded there and then.
- If there are any controversial aspects of the content of a client's file, legal advice must be sought. This might be where there is a court case between parents or where social care or the police may be considering legal action, or where a case has already completed, and an appeal process is underway.
- A setting should never 'under-record' for fear of the parent/carer seeing, nor should they make 'personal notes' elsewhere.

Further guidance

The Information Commissioner's Office https://ico.org.uk/ or helpline 0303 123 1113.

9. Transfer of records

EYA Policy Template Reference: 07.4

Records about a child's development and learning in the EYFS are made by staff at Longparish Little School; to enable smooth transitions, appropriate information is shared with the receiving setting or school at transfer. Confidential records are passed on securely where there have been concerns, as appropriate.

Transfer of development records for a child moving to another early years setting or school

- It is the setting manager's responsibility to ensure that records are transferred and closed in accordance with the archiving procedures, set out below.

- Safeguarding records and reports are transferred confidentially to the new setting, and the person receiving the records must sign to say they have been received. Once passed over, these then become the property of the new setting.

Development and learning records

- The key person prepares a summary of achievements in the prime and specific areas of learning and development
- This record refers to any additional languages spoken by the child and their progress in all languages.
- The record also refers to any additional needs that have been identified or addressed by the setting and any action plans.
- The record also refers to any special needs or disability and whether early help referrals, or child in need (CIN) referrals or child protection (CP) referrals, were raised in respect of special educational needs or disability, whether there is an Action Plan (or other relevant plan, such as CIN or CP, or early help) and gives the name of the lead professional.
- The summary shared with schools should also include whether the child is in receipt of, or eligible for EYPP (Early Years Pupil Premium) or other additional funding.
- The record contains a summary by the key person and a summary of the parent/carers' view of the child.
- The document may be accompanied by other evidence such as photos or drawings that the child has made.
- The setting will use the local authority's assessment summary format or transition record, where these where provided.
- Whichever format of assessment summary is used, it should be completed and shared with the parent/carer prior to transfer.

Transfer of confidential safeguarding and child protection information

- The receiving school/setting will need a record of child protection concerns raised in the setting and what was done about them. The responsibility for transfer of records lies with the originating setting, not on the receiving setting/school to make contact and request them.
- To safeguard children effectively, the receiving setting must be made aware of any current child protection concerns, preferably by telephone, prior to the transfer of written records.

- Parents/carers should be reminded that sensitive information about their child is passed onto receiving settings where there have been safeguarding concerns and should be asked to agree to this prior to the information being shared. Settings are obliged to share data linked to “child abuse” which is defined as physical injury (non-accidental) physical and emotional neglect, ill treatment and abuse.
- Parents/carers should be asked to agree to this, however, where safeguarding concerns have reached the level of a referral being made to local children’s social work services (either due to concerns that a child may be at risk of significant harm or that a child may be in need under Section 17 of the Children Act,) if consent is withheld the information will most likely need to be shared anyway. It is important that any decisions made to share or not share with or without consent are fully recorded.
- For any safeguarding or welfare concerns that resulted in an early help referral being made, and if consent to share is withheld, legal advice is sought prior to sharing.
- If the level of a safeguarding concern has not been such that a referral was made for early help, or to children’s social work services or police, the likelihood is that any concerns were at a very low level and if they did not meet the threshold for early help, they are unlikely to need to be shared as child abuse data with a receiving setting, however, the designated safeguarding lead should make decisions on a case by case basis, seeking legal advice as necessary.
- The designated safeguarding lead person should check the quality of information to be transferred prior to transfer, ensuring that any information to be shared is accurate, relevant, balanced and proportionate. Parents/carers can request that any factual inaccuracies are amended prior to transfer.
- If a parent/carer wants to see the exact content of the safeguarding information to be transferred, they should go through the subject access request process. It is important that a child or other person is not put at risk through information being shared.
- If no referrals have been made for early help or to children’s social work services and police, there should not normally be any significant information which is unknown to a parent/carer being shared with the receiving school or setting.
- If a parent/carer has objections or reservations about safeguarding information being transferred to the new setting, or if it is unclear what information should be included, the designated person will seek legal advice.
- If LSP requirements are different to the setting’s this must be explained to the parent/carer, and a record of the discussion should be signed by parents/carers to

indicate that they understand how the information will be shared, in what circumstances, and who by.

- Safeguarding records and reports are transferred confidentially to the new setting, and the person receiving the records must sign to say they have been received. Once passed over, these then become the property of the new setting.
- If a child protection plan or child in need plan is in place, **Safeguarding Concerns Monitoring Form (see Safeguarding Policies – Forms)** is also photocopied and a copy is given to the receiving setting or school, along with the date of the last professional meeting or case conference.
- If a S47 investigation has been undertaken by the local authority a copy of the child welfare and protection concern summary form is given to the receiving setting/school.
- Where a CAF (Common Assessment Framework)/early help assessment has been raised in respect of welfare concerns, the name and contact details of the lead professional are passed on to the receiving setting or school**.**
- If the setting has a copy of a current plan in place due to early help services being accessed, a copy of this should be given to the receiving setting, with parental consent.
- Where there has been a S47 investigation regarding a child protection concern, the name and contact details of the child's social worker will be passed on to the receiving setting/school, regardless of the outcome of the investigation.
- Where a child has been previously or is currently subject to a child protection plan, or a child in need plan, the name and contact details of the child's social worker will be passed onto the receiving setting/school, along with the dates that the relevant plan was in place for.
- This information is posted (by 'signed for' delivery) or taken to the school/setting, addressed to the setting's or school's designated person for child protection and marked confidential. Electronic records must only be transferred by a secure electronic transfer mechanism, or after the information has been encrypted.
- Parent/carers should be made aware what information will be passed onto another setting via **Privacy Notice.**
- Copies of the last relevant initial child protection conference/review, as well as the last core group or child in need minutes can be given to the setting/school.

- The setting manager must review and update **Safeguarding Concerns Monitoring Form (Safeguarding Policies – Forms)**, checking for accuracy, proportionality, and relevance, before this is copied and sent to the setting/school.
- The setting manager ensures the remaining file is archived in line with the procedures set out below.

  No other documentation from the child's personal file is passed to the receiving setting or school. The setting keeps a copy of any safeguarding records in line with required retention periods.

Archiving children's files

- All records to be retained are scanned and stored on Famly. All original documents are disposed of through confidential waste collection.
- For web-based or electronic children's files, the designated person must also use the archiving procedure, and records details of what needs to be retained/destroyed. The designated person must plan to ensure that electronic files are deleted/retained as required in accordance with the required retention periods in the same way as paper-based files.
- Health and safety records and some accident records pertaining to a child are stored in line with required retention periods.

10. Data Breach Procedure

What is a Personal Data Breach?
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): –

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an email or SMS to the wrong recipient).
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

When does It need to be reported?

Longparish Little School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: –

- Potential or actual discrimination.
- Potential or actual financial loss.
- Potential or actual loss of confidentiality.
- Risk to physical safety or reputation.
- Exposure to identity theft (for example through the release of non-public identifiers such as passport details).
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should contact the Data Protection Officer, Sally Lawman as soon as possible and within 72 hours.

Breach reporting is encouraged throughout Little School and staff are expected to report any incident, even if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals.

Once reported, you should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators or investigate further. Claire Nash will acknowledge receipt of the data breach report and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording the Breach

On being notified of a suspected personal data breach, Sally Lawman will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:

- Where possible, contain the data breach.
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed.
- Assess and record the breach in the preschool's data breach register.
- Notify the ICO.

- Notify data subjects affected by the breach.
- Notify other appropriate parties to the breach.
- Take steps to prevent future breaches.

Notifying the ICO

Sally Lawman will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.
This will be done without undue delay and within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (I.e. it is not 72 working hours). If Little School is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, Sally Lawman will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures Little School has (or intends) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, Claire Nash will co-operate with and seek guidance from the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the Little School website).

Notifying Other Authorities
Little School will need to consider whether other parties need to be notified of the breach. For example:

- Insurers.
- Parents.
- Third parties (for example when they are also affected by the breach).
- Local authority.
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing the Breach

Once initial reporting procedures have been carried out, Little School will carry out all necessary investigations into the breach.

Little School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: –

- What type of data is involved and how sensitive it is.
- The volume of data affected.
- Who is affected by the breach (i.e. the categories and number of people involved).
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise.
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation).
- What has happened to the data.
- What could the data tell a third party about the data subject.
- What are the likely consequences of the personal data breach on the school.
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, Little School will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what security measures were in place when the breach occurred.
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again.
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice.
- Consider whether it is necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken.
- To update the data breach register.
- To debrief the committee/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to Sally Lawman. This can help capture risks as they emerge, protect Little School from data breaches and keep our processes up to date and effective.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to Little School.

11. Reserves Policy

Policy statement

The Committee has reviewed Longparish Little School's need for reserves in line with guidance issued by the Charity Commission and the Early Years Alliance. Reserves can be categorised as **General** or **Specific**.

GENERAL RESERVE

Longparish Little School needs a General Reserve in order to:

1. Meet redundancy liabilities should the Little School have to close.
2. Ensure continuity of service provision by:
    - Meeting unexpected costs such as cover for illness or maternity leave etc;
    - Covering running costs during periods of lower income (e.g. while adjusting to school policy changes or following falls in fundraising).
3. Replace equipment as it wears out and carry out necessary building maintenance.
4. Re-locate the Little School from the building owned by Longparish School.

Therefore, Longparish Little School aims to maintain reserves consisting of:

- Reserves to meet redundancy liabilities calculated annually using https://www.gov.uk/calculate-your-redundancy-pay (last calculated 16 July 2025) – this amount to cover contractual notice period (min 4 weeks, max 12 weeks) and statutory redundancy pay (1 week per year to 12 weeks)
- Running costs for at least one term

- Commercial rental costs for at least one term, should the Little School need to relocate

The total sum held in General Reserves for 2025/26 is **£52,500.00**

The Committee believes that this level of reserves is prudent and necessary to ensure that Longparish Little School can run efficiently and meet future needs.

"All groups are recommended to have at least three months' expenditure in reserve and a sum which covers the calculated redundancy liability" (Managing a Charitably Constituted Setting, Early Years Alliance)

"As a guide, many groups choose one term's reserves as a suitable level" (Finance in Early Years Settings, Early Years Alliance)

SPECIFIC RESERVES

It is intended that income generated from fund-raising activities will be added to the Reserve account and earmarked for specific purposes.

Purposes of Specific Reserves:

• Renewals – to enable Little School to plan and finance an effective programme of equipment replacement and planned property maintenance. These reserves are a mechanism to smooth expenditure so that a sensible replacement programme can be achieved without the need to vary budgets dramatically from year to year.

• Carry forward of underspend - expenditure committed to a project but not spent in the budget year. Reserves can be used as a mechanism to carry forward this resource.

• Other Specific Reserves may be set up from time to time to meet known or predicted liabilities.

Where the purpose of a Specific Reserve becomes obsolete, or where there is an over-provision of funds, the excess may on the approval of the Committee be transferred to other budget headings within the revenue budget or to General Reserves or to one or more other Specific Reserves.

Specific Reserves 2025/26

Little School aims to raise funds for the creation of a Sensory Classroom pod at Little School.

Monitoring of Reserves

The Committee will monitor the actual level of reserves and compare with the target level no less than once a year (at the financial year end). Longparish Little School has no restricted funds, and therefore essentially all cash balances can be considered to be part of reserves.

Balance falls below target level

In the event of reserves falling significantly below the target level, Longparish Little School will aim to restore the reserves as soon as possible by;

- increasing fundraising,
- increasing earned income,
- and reducing expenditure.

Balance is above target level

If reserves are significantly above the target level, the Committee will put in place a plan as soon as possible, aiming to eliminate the excess within four years by;

- spending money to enhance the quality of provision, or otherwise further the aims of Little School, or
- by reducing fund-raising.

The Committee will not take any steps that might call into question the ability of Longparish Little School to continue as a financially viable operation in the long term. In particular, it will not plan to use excess reserves to cover essential running costs.