



DATA PROTECTION POLICIES September 2023

I. CONFIDENTIALITY AND ACCESS TO RECORDS

POLICY STATEMENT

Definition: 'Confidential information is information of some sensitivity, which is not already lawfully in the public domain or readily available from another public source, and which has been shared in a relationship where the person giving the information understood it would not be shared with others.'

(INFORMATION SHARING: PRACTITIONERS' GUIDE)

In our school, staff can be said to have a 'confidential relationship' with families. It is our intention to respect the privacy of children and their parents and carers, while ensuring that they have access to high quality care and education in our setting. We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the Data Protection Act and the Human Rights Act.

1. Confidentiality procedures

Notification:

Our data processing activities are registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:

<https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/>

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: <https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/>

The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data.

Notifications shall be [in accordance with ICO guidance](#) and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for 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 an individual's data shall first be notified to them.

Under no circumstances will the school disclose information or data:



- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions without the parents consent.

Data Security:

In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance [with guidance given by the ICO](#).

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Natasha Henderson-Stewart

La Petite Ecole Bilingue - Stewart Bilingual School

22 VICAR'S ROAD

NW5 4NL London



No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- **Other schools**

If a pupil transfers from La Petite Ecole Bilingue to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

- **Examination authorities**

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

- **Health authorities**

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

- **Police and courts**

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

- **Social workers and support agencies**

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

- **Educational division**

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Right to be Forgotten:

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only.

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

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

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school files but accessible to the first aider.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have off site meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced, they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal service.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with [ICO guidance](#).

The school uses Shred-it to dispose of sensitive data that is no longer required.

Legal framework

<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> 2018

Further guidance

'Information sharing: advice for practitioners providing safeguarding services (2018)'.
<https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice>

II. INFORMATION SHARING

"Information sharing is essential for effective safeguarding and promoting the welfare of children and young people. It is a key factor identified in many serious case reviews (SCRs), where poor information sharing has resulted in missed opportunities to take action that keeps children and young people safe."

['Information sharing: advice for practitioners providing safeguarding services \(2018\)'](#).

POLICY STATEMENT

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

We are obliged to share confidential information without authorisation from the person who provided it or to whom it relates if it is in the public interest. That is when:

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

The decision should never be made as an individual, but with the back-up of the Head Teacher and/or Proprietor. The three critical criteria are:

- Where there is evidence that the child is suffering, or is at risk of suffering, significant harm.
- Where there is reasonable cause to believe that a child may be suffering, or 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.

PROCEDURES

Our procedure is based on the 7 golden rules for information sharing as set out in [Information sharing: advice for practitioners providing safeguarding services \(2018\)](#)

1. Remember that the **Data Protection Act** is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.
2. Be open and honest.

- Explain to families how, when and why information will be shared about them and with whom. **See Privacy notice at Appendix 1**
 - Seek consent to share information, unless it puts the child at risk or undermines a criminal investigation.
 - In our school we ensure parents/carers:
 - Receive information about our information sharing policy when starting their child in the setting, and sign a form to say that they understand circumstances when information may be shared without their consent. This will only be when it is a matter of safeguarding a child or vulnerable adult. This is on our registration form;
 - Have information about our Safeguarding Children and Child Protection policy;
 - Have information about the circumstances when information will be shared with external agencies, for example, with regard to any special needs the child may have or transition to school.
3. Seek advice when there are doubts about possible significant harm to a child or others.
- The leadership team contact children's social care for advice where they have doubts or are unsure.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared.

Respect the wishes of children and parents not to consent to share confidential information. However, in the interests of the child, know when it is reasonable to override their wish.

5. Consider safety and well-being: base information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions. The school leadership team are conversant with this and are able to advise staff accordingly. We consider the safety and welfare of the child when making a decision about sharing information – if there are concerns regarding 'significant harm' the child's well-being and safety is paramount.

In our school we:

- Record concerns and discuss these with the school's designated person for child protection matters;
 - Record decisions made and the reasons why information will be shared and to whom; and
 - Follow the procedures for reporting concerns and record keeping.
6. Information shared should be accurate and up-to-date, necessary for the purpose it is being shared for, shared only with those who need to know and shared securely.

- Our Child Protection procedure set out how and where information should be recorded and what information should be shared with another agency when making a referral.
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

CONSENT

Parents have a right to be informed that their consent to share information will be sought in most cases, as well as the kinds of circumstances when their consent may not be sought, or their refusal to give consent may be overridden. We do this as follows:

- Our policies and procedures set out our responsibility regarding gaining consent to share information and when it may not be sought or overridden.
- We may cover this verbally when the child starts or include this in our prospectus.
- Parents sign a form at registration to say they understand this.
- Parents are asked to give written consent to share information about any additional needs their child may have, or to pass on child development summaries, to the next provider/school.
- Copies are given to parents of the forms they sign.

The principles

The principles set out below are intended to help practitioners working with children, young people, parents and carers share information between organisations. Practitioners should use their judgment when making decisions about what information to share, and should follow organisation procedures or consult with their manager if in doubt.

The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child.

Necessary and proportionate

When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than is necessary to be of use is a key element of the GDPR and Data Protection Act 2018, and you should consider the impact of disclosing information on the information subject and any third parties.

Information must be proportionate to the need and level of risk.

Relevant Only

Information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

Adequate

Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young person at increased risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure

Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

Record Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary.

In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so

We consider the following questions when we need to share:

- Is there a legitimate purpose to sharing the information?
- Does the information enable the person to be identified?
- Is the information confidential?
- If the information is confidential, do you have consent to share?
- Is there a statutory duty or court order to share information?
- If consent is refused, or there are good reasons not to seek consent, is there sufficient public interest to share information?
- If the decision is to share, are you sharing the right information in the right way?
- Have you properly recorded your decision?



All the undertakings above are subject to the paramount commitment of the school, which is to the safety and well-being of the child.

Legal framework

Data Protection Act 2018

Human Rights Act 1998

Further guidance

Information Sharing: Guidance for Practitioners and Managers

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

Appendix 1

PRIVACY NOTICE FOR PARENTS AND PUPILS

LPEBL is committed to protecting the privacy and security of personal information. This privacy notice describes how we collect and use personal information about pupils, in accordance with the General Data Protection Regulation (UK GDPR), section 537A of the Education Act 1996 and section 83 of the Children Act 1989.

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.

Who Collects This Information

The Head Teacher oversees this role. This means that we are responsible for deciding how we hold and use personal information about pupils and parents.

The Categories of Pupil Information That We Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you and/or your child:

- Personal information such as name, pupil number, date of birth, gender and contact information;
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses;
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Details of previous / future schools and UPN (Unique Pupil Number);
- Attendance details (such as sessions attended, number of absences and reasons for absence);
- Performance and assessment information;
- Behavioural information (including exclusions);
- Special educational needs information;
- Relevant medical information;
- Images of pupils engaging in school activities, and images captured by the School's CCTV system;
- Recordings of pupils and/or parents from the School's video conferencing platform;



- Information about the use of our IT, communications and other systems, and other monitoring information;
- Special categories of personal data (including ethnicity, relevant medical information, special educational needs information, religious beliefs, information relating to keeping you safe, Religious/Cultural or medical dietary requirements);

Collecting This Information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

How We Use Your Personal Information

We hold pupil data and use it for:

- Pupil selection (and to confirm the identity of prospective pupils and their parents)
- Providing education services and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Informing decisions such as the funding of schools;
- Assessing performance and to set targets for schools;
- Safeguarding pupils' welfare and providing appropriate pastoral (and where necessary medical) care;
- Support teaching and learning;
- Managing internal policy and procedure;
- Enabling pupils to take part in assessments, to publish the results of examinations and to record pupil achievements;
- To carry out statistical analysis for diversity purposes;
- Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care;
- Enabling relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- Making use of photographic images of pupils in school publications, on the school website and on social media channels;
- Security purposes, including CCTV; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

Collecting Data for Test and Trace

In the current pandemic, we may need to store your data for test and trace purposes. This is in order for the school to engage with the test and trace process, make decisions on safety within the school and whether individuals are required to self-isolate or carry out a test. To do this we may be recording your name, contact number and date and time of arrival as well as time of departure. To complement the above we may also ask for data that has not previously supplied. This will allow us to assess an individual's ability to attend/return to school and what measures may need to be put in place to allow for a safe return. We, additionally, may need to collect data about individuals that you reside with in order to factor in appropriate considerations for their wellbeing. All data collected by the school will be processed in accordance with our retention, destruction, data protection and data security policies. All data collected for test and trace purposes will be retained for 21 days in accordance with government guidelines. The legal bases for using your data in these circumstances will be for the reasons of substantial public interest and in the interests of public health. Dependant on circumstances the basis may be to assess the working capacity of an employee or to protect the vital interests of yourself or another person. We may need to share select data with others. This can be with the NHS and emergency services, public health, public authorities as well as other stakeholders. This will only be done where it is necessary and proportionate for us to do so.

The Lawful Basis on Which We Use This Information

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life. •Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and
- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

Sharing Data

We may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it's the only way we can make sure you stay safe and healthy or we are legally required to do so. We share pupil information with:

- the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- Ofsted or ISI;
- Other Schools that pupils have attended/will attend;
- NHS;
- Welfare services (such as social services);
- Law enforcement officials such as police, HMRC;
- Local Authority Designated Officer;
- Professional advisors such as lawyers and consultants;
- Support services (including insurance, IT support, information security); and
- The Local Authority.

Information will be provided to those agencies securely or anonymised where possible. The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Why We Share This Information

We do not share information about our pupils with anyone without consent unless otherwise required by law. For example, we share students' data with the DfE on a statutory basis which underpins school funding and educational attainment. To find out more about the data collection requirements placed on us by the DfE please go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

Storing Pupil Data

The School keeps information about pupils on computer systems and sometimes on paper. Except as required by law, the School only retains information about pupils for as long as necessary in accordance with timeframes imposed by law and our internal policy. Full details on how long we keep personal data for is set out in our record keeping policy.

Automated Decision Making

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in limited circumstances. Pupils will not be subject to automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way).

The National Pupil Database

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies. We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013. To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>. The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
 - the purpose for which it is required
 - the level and sensitivity of data requested: and
 - the arrangements in place to store and handle the data
- To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.



For more information about the department's data sharing process, please visit:
<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
<https://www.gov.uk/government/publications/national-pupil-database-requests-received>
To contact DfE: <https://www.gov.uk/contact-dfe>
Requesting Access to Your Personal Data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information please contact the Head Teacher.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress;
 - Prevent processing for the purposes of direct marketing;
 - Object to decisions being taken by automated means;
 - In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed;
- and
- Claim compensation for damages caused by a breach of the data protection regulations.

If you want to exercise any of the above rights, please contact the Head Teacher in writing. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to Withdraw Consent

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Head Teacher. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Contact

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with the Head Teacher in the first instance. We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Head Teacher then you can contact the DPO on the details below:



-Data Protection Officer: Natasha Henderson-Stewart
Address: 22 Vicars Road NW5 4NL
Email: nhs@lpebl-kt.com

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues at <https://ico.org.uk/concerns>.

Changes to This Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

III. RECORD KEEPING

1. Children's records

POLICY STATEMENT

There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the Data Protection Act and the Human Rights Act.

This policy and procedure is taken in conjunction with the Confidentiality Policy and our procedures for information sharing.

PROCEDURES

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

a. Developmental records

These include observations of children in the setting, photographs, video clips and samples of their work and summary developmental reports.

These are usually kept in the classroom and can be freely accessed, and contributed to, by staff, the child and the child's parents.

b. Personal records

These include registration and admission forms, signed consent forms, and correspondence concerning the child or family, reports or minutes from meetings concerning the child from other agencies, an on-going 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.

These confidential records are stored in a lockable file or cabinet and are kept secure by the person in charge in an office or other suitably safe place.

Parents have access, in accordance with our Client Access to Records policy, to the files and records of their own children but do not have access to information about any other child.

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.

We retain children's records for three years after they have left the setting. These are kept in a secure place.

c. Other records

Issues to do with the employment of staff, whether paid or unpaid, remain confidential to the people directly involved with making personnel decisions.
Students - including those on work-experience - when they are observing in the setting, are advised of our confidentiality policy and are required to respect it.

Legal Framework

Data Protection Act 2018
Human Rights Act 1998

Further guidance

Information Sharing: Guidance for Practitioners and Managers (DCSF 2018)

2. School's own records

POLICY STATEMENT

We keep records for the purpose of maintaining our school. These include:

- Lease documents and other contractual documentation pertaining to amenities, services and goods. (Proprietor)
- Financial records pertaining to income and expenditure. (Financial Officer)
- Risk assessments.
- Employment records of staff. (Office Manager)
- Training records of staff
- Performance management

Our records are regarded as confidential on the basis of sensitivity of information, such as with regard to employment records and these are maintained with regard to the framework of the Data Protection Act and the Human Rights Act.
This policy and procedure is taken in conjunction with the Confidentiality and Client Access to Records policy and Information Sharing policy.

PROCEDURES

All records are the responsibility of the Head Teacher, Office Manager, Financial officer or Owner who ensures they are kept securely.

All records are kept in an orderly way in files and filing is kept up-to-date. Financial records are kept up-to-date for audit purposes by the Finance Officer.

Health and safety records are maintained; these include risk assessments, details of checks or inspections and guidance etc.

All our employment and staff records are kept securely and confidentially.

Practice Guidance

Schools' Recording of Child Protection Concerns Background

Ofsted studied a series of serious case reviews and identified school record keeping as an important factor in keeping children safe.

Their review said " Specific concerns about school records were noted in 15 of the 50 evaluations in relation to the adequacy and accuracy of records, and in four cases it was noted that school records had been lost."

And on recording incidents, issues and concerns over time " There were some good examples of schools keeping a record over time, but the significance of the information had not been recognised. In other cases school records were poor even when a child was subject to a formal monitoring process, such as those with a statement of special educational needs."

As a result the section 5 guidance on safeguarding inspection by ofsted includes the requirement that..... "inspectors should take into account the extent to which the school records information relevant to safeguarding concerns clearly and accurately and shares it appropriately, both internally and with other agencies"

This should be done by "evaluating the quality of recording, by reviewing at least one case file of a pupil where there have been child protection concerns."

Structure and Content of Files

- Each child for whom there has been any cp concern from a minor suspicion years ago to an ongoing case where a child is subject to a cp plan should have a cp file that is separate from their school education file.
- The child protection file has a separate legal status from pupil education files.
- The file should contain all papers from a note of a teacher's concern to conference minutes
- Inside the front cover should be a chronology and index showing all documents, incidents, consultation with social care or child protection advisors, referrals, meeting



attended, decisions taken, notes of any review of the pupils progress undertaken at school, which staff are told about a pupil's case and why and any role they are to take in the response to the concern.

- The chronology has a crucial role in allowing current and future staff to get an overview of the case so that any new development can be assessed in the correct context.
- The file should reflect that it is a tool for monitoring and implementing a pro-active management of the child protection case in the school.
- Quality of recording. See attached ofsted appendix Transfer of Files There is a duty for schools to transfer a copy of any child protection file to any new school that the pupil joins. This applies even if the case is closed.

The file should be transferred from designated teacher to designated teacher.
Management of Files

- Files should be kept in a locked cabinet to which the designated teacher controls access.
- Files should be cross-referenced to the school education file so that current and future staff can know there is a child protection file.
- Schools should maintain a list of vulnerable pupils and child protection concerns should be a category of vulnerability.

Long Term Storage of Files

There is no clear guidance on how long schools should store child protection files. However, files may be needed for a variety of purposes.

They may need to be linked to concerns about younger siblings.

They may be needed for future court hearings either in the family proceedings court or civil action for compensation. They may be needed for future serious case reviews.

For all these reasons it is best to store the file permanently, pending any further national guidance on storage times.

Files can be scanned and saved electronically.

The LA can advise on agencies and costs involved in this process.

Appendix 1 OFSTED GUIDANCE ON RECORDING

Evaluating the quality of records relating to safeguarding issues Possible questions to consider – this is not a definitive list.

Are records up to date and complete?

Do records demonstrate both effective identification and management of the risk of harm?

Do records demonstrate sound decision-making, appropriate responses to concerns and evidence of relevant referrals made in a timely manner?

Do they indicate that appropriate action is taken in response to concerns and allegations in a timely manner?

Do they show evidence of tenacity in following up concerns with relevant agencies?

Do they provide evidence of effective partnership working and sharing of information?

Is there evidence of attendance at or contribution to inter-agency meetings and conferences?

Is there clarity about the school's policy relating to the sharing of information internally, safe keeping of records, and transfer when a pupil leaves the school?

Legal framework

Data Protection Act 1998

Human Rights Act 1998

Ofsted guidance on recording

Date of adoption of this policy	2 September 2023
Date of last review of this policy	18 August 2023
Date for next review of this policy	18 August 2024
Policy owner (SLT)	Headteacher and DSL
Authorised by	Headteacher, DSL and Proprietor