La Petite Ecole Française
73 Saint Charles Square
London W10 6EJ
Tel: 0208 960 1278
E-mail: LaPetiteEcoleFrancaise@gmail.com
Directrice de l'école: Camie Steuer
Directrice Administrative: Sarah Silvestre

DATA PROTECTION POLICY

Introduction and Scope

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 are the laws governing the processing of personal data in the United Kingdom. They apply to anyone that uses or accesses personal data. This policy sets out how La Petite Ecole Française (LPEF) processes personal data and complies with the legislation and covers all processing of personal data whether in electronic or paper formats.

La Petite Ecole Française (LPEF) is a Data Controller registered with the Information Commissioner's Office (ICO) and must comply with the regulations in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The school must be able to demonstrate compliance. Failure to comply exposes the school to civil claims and/or enforcement action from the ICO that may include financial penalties.

Staff, when processing personal data for school business, are acting on behalf of the Data Controller, and for avoidance of doubt, when this policy refers to actions the school shall take, it also means the staff involved with the processing of relevant personal data. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school. Any failures to follow this policy may result in disciplinary proceedings.

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller (this is the school LPEF)	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Proprietor Devika Malik - Data Compliance Lead

The Proprietor, Devika Malik, has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Deputy Head and Headteacher

The Deputy Head and Headteacher act as the representative of the 'data compliance lead' on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Deputy Head or Headteacher in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

• The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
• The data needs to be processed so that the school can comply with a legal obligation
• The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
• The data needs to be processed so that the school can perform a task in the public interest, and carry out its official functions
• The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
• The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management.

8. Accurate data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. Timely processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

10. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this unless it is a safeguarding concern.
- We may share the names of pupils with other AEFE schools in London for educational progression purposes.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

• The prevention or detection of crime and/or fraud
• The apprehension or prosecution of offenders
• The assessment or collection of tax owed to HMRC
• In connection with legal proceedings
• Where the disclosure is required to satisfy our safeguarding obligations
• Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

11. Subject access requests

LPEF's procedures for responding to formal requests from a data subject for information that the school holds about them is set out in Appendix 1.

12. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

13. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the School Office.

14. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. **We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.** We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

• Within school on notice boards and in school magazines, brochures, newsletters, etc.
• Outside of school by external agencies such as the school photographer, newspapers, campaigns
• Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

• Appointing a Data Compliance Lead, and ensuring that staff have the necessary resources to fulfil their duties and maintain their knowledge

• Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
• Integrating data protection into internal documents including this policy, any related policies and privacy notices
• Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
• Maintaining records of our processing activities, including:
For the benefit of data subjects, making available the name and contact details of our school and all information we are required to share about how we use and process their personal data (via our privacy notices). An email is sent to parents annually.

16. Processing in line with data subject's rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- transparency of data processing by being informed of how their data is processed;
- request access to any data held about them by a data controller;
- prevent the processing of their data for direct-marketing purposes;
- ask to have inaccurate data amended;
- object to any decision that significantly affects them being taken solely by a computer or another automated process;
- ask for personal data not to be processed where it is processed on the basis of LPEF's legitimate interest unless there are compelling legitimate grounds which override the interests, rights and freedoms of the data subject;
- ask for personal data in a structured and machine readable format and to transfer it to another data controller without hindrance from LPEF (data portability) if the processing is carried out by automated means and the legal basis for processing is consent or contract;
- ask for personal data to be erased provided that the personal data is no longer necessary for the purposes for which it was collected, consent is withdrawn (if the legal basis for processing is consent), and there are no overriding legitimate ground for processing, the personal data is unlawfully processed, the data needs to be erased to comply with a legal obligation or the personal data is children's data and was collected in relation to an offer of information society services;
- to ask for the processing of that information to be restricted if the accuracy of that data is contested, the processing is unlawful, the personal data is no longer necessary for the purposes for which it was collected or if the right to object is exercised (pending verification of whether there are legitimate grounds for processing); and
- ask for the personal data not to be processed for scientific or historical research purposes, where relevant, unless the processing is necessary in the public interest.

17. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:
• Paper-based records are kept under lock and key and portable electronic devices, such as laptops and hard drives that contain personal data have a secure password
• Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
• Personal information should not be taken off site
• Passwords are used to access school computers, laptops and other electronic devices.
• Staff who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment

18. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

19. Providing information to third parties

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by the school. In particular they should:

- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested.
- Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified.
- Refer to the Proprietor, Headteacher or Deputy Head for assistance in difficult situations.
- Where providing information to a third party, do so in accordance with the data protection principles (No.6).

20. Providing information over the telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information by the school. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Request assistance from the Proprietor, Headteacher or Deputy Head in difficult situations. No-one should be bullied into disclosing personal information.

21. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

• Safeguarding information being made available to an unauthorised person
• The theft of a school laptop containing non-encrypted personal data about pupils

22. Monitoring arrangements

The Proprietor (Data Compliance Lead) is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary, when there are any changes to the law that affect our school's practice. Otherwise, this policy will be reviewed every year.

23. Links with other policies

This data protection policy is linked to our:

• E-Safety and Acceptable Use Policy
• Policy on use of Mobile Phones, Cameras and Recording Devices
• Staff Code of Conduct
• Safeguarding Children Policy

APPENDIX 1: Procedure for Subject Access Requests

Making a subject access request
An individual is only entitled to access their own personal data, and not to information relating to other people. Subject access requests must be submitted in writing, either by letter or email to the school. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the Headteacher or Deputy Head.

An individual has the right to request any and all personal data held (subject to the exclusions set out below). If a request is broad, staff can request further information to narrow the personal data requested, however the individual has no obligation to narrow the request. The time limit for providing a response shall run from the time of the original request and is not affected by staff requests to narrow the information requested in the subject access request.

Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Cost
The subject access request must be dealt with free of charge unless it is manifestly unfounded or excessive or requests multiple copies of the same information, in which case a reasonable fee may be charged taking into account administrative costs of providing the information.

Identification of individuals
LPEF is also entitled to request information to judge whether the person making the request is the individual to whom the personal data relates and/or is a person with parental responsibility for a child whose data is the subject of the request. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception. Evidence of identity may be established by production of:

- passport
- driving licence
- utility bills and or bank statements with the current address
- birth certificate
- P45/P60
- credit card or mortgage statement
- May contact the individual via phone to confirm the request was made

RESPONDING TO A SUBJECT ACCESS REQUEST
The response time for subject access requests, once officially received, is 1 calendar month. However, if

a request is sent to the school during a school holiday the school will be closed and the request will not be received until the first day after the school holiday. If the request is received within a month prior to a school holiday and it is not possible for the request to be dealt with before the school holiday commences, the school will inform the requester that the 1 month deadline for the request will be extended by the length of the school closure. As set out above, the 1 calendar month will not commence until after receipt of evidence of identity where LPEF has reasonable doubts as to the identity of the requesting individual. That period may be extended by two further calendar months where necessary taking into account the complexity and number of the requests. Where the period is extended, LPEF will inform the data subject of the extension and the reasons for the extension within 1 calendar month of receipt of the request. LPEF shall always endeavour to respond to subject access requests without utilising this extension period.

We will not disclose information if it:

• Might cause serious harm to the physical or mental health of the pupil or another individual
• Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
• Is contained in adoption or parental order records
• Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

When responding to a subject access request, LPEF will:

- acknowledge receipt of the request and provide an indication of the likely timescale for a response within 14 working days;
- take all reasonable and proportionate steps to identify and disclose the data relating to the request;
- never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events;
- consider whether to seek consent from any third parties which might be identifiable from the data
- being disclosed;
- seek legal advice, where necessary, to determine whether we are required to comply with the request or supply the information sought;
- provide a written response, including an explanation of the types of data provided and whether and for what reasons any data has been withheld; and
- ensure that information disclosed is clear and technical terms are clarified and explained.

Circumstances when we may refuse or limit a subject access request

LPEF is not required to comply with a subject access request in relation to:

- confidential references given by LPEF for employment or educational purposes;
- personal data processed in connection with management forecasting or planning if it would prejudice the conduct of the business of LPEF;
- personal data subject to legal professional privilege;
- information which may cause serious harm to the physical or mental health or emotional condition of a child or another, or which would reveal that a child is at risk of abuse, or information relating
- to court proceedings.

LPEF is also not required to supply the information requested if:

- the data requested is not available;
- the information is subject to legal professional privilege;
- an identical or similar request has been made by the same individual previously, unless a reasonable interval has elapsed between the previous and the current request; in determining whether a 'reasonable interval' has elapsed, LPEF will have regard to the nature of the data, the purpose for which the data is processed and the frequency with which the data is altered;
- LPEF cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless:

  1) the other individual has consented to the disclosure of the information, or
  2) it is reasonable in all the circumstances to comply with the request without the consent of the other individual; in determining whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, LPEF shall have regard to any duty of confidentiality owed to the other individual and any express refusal of consent by the other individual.

In order to provide the whole or some of the information requested, LPEF may undertake redaction (information blacked out/removed) of one or more documents. An explanation of why information has been redacted will be provided.

Appendix 2: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Headteacher or Deputy Head, who will immediately inform the Proprietor
- The Proprietor will investigate the report, and determine whether a breach has occurred. To decide, the Proprietor will consider whether personal data has been accidentally or unlawfully been:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The Proprietor will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. The Proprietor will assess the potential consequences, based on how serious they are, and how likely they are to happen

The Proprietor will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Proprietor will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

o Loss of control over their data
o Discrimination
o Identify theft or fraud
o Financial loss
o Damage to reputation

o Loss of confidentiality
o Any other significant economic or social disadvantage to the individual(s) concerned
If it's likely that there will be a risk to people's rights and freedoms, the Proprietor must notify the ICO.

The Proprietor will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Where the ICO must be notified, the Proprietor will do this via the 'report a breach' page of the ICO website within 72 hours.

As required, the Proprietor will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the Proprietor
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the Proprietor will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Proprietor expects to have further information. The Proprietor will submit the remaining information as soon as possible

The Proprietor will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Proprietor will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the Proprietor
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
  - If possible, the Proprietor will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The Proprietor will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The Proprietor, Headteacher and Deputy Head will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

• If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
• Members of staff who receive personal data sent in error must alert the sender and the Proprietor as soon as they become aware of the error
• In any cases where the recall is unsuccessful, the Proprietor will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
• The Proprietor will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

Sensitive information being disclosed via school website
• Member of staff who discovers the sensitive information to inform the Headteacher or Deputy Head as soon as possible, and they will intern inform the Proprietor immediately.
• Proprietor to arrange for information to be removed from the school website immediately.
• Parents to be informed that sensitive information was available on the website and that action has been taken to remove it.
• Proprietor to follow data breach protocols.