International School of Paris - Privacy Policy

Last updated 14th December 2018

The International School of Paris is very aware of the importance of privacy and data protection and would like to share with you some details of how we process and protect your personal data in a way that is compliant with the new General Data Protection Regulation (GDPR).

This Privacy Notice applies to all individuals who share data with us whether they are parents, students, prospective students, staff, visitors to the school, or even just visitors to our website.

In the language of GDPR, The International school of Paris is the Data Controller and you are the Data Subject. To help you understand how we process the data that is within our control we have arranged this document in the following sections:

1. What categories of personal data are collected and processed?
2. Why is the data collected and how is the data used?
3. What is our lawful basis for processing the data?
4. How the is data collected, stored, for how long and how is security ensured?
5. Who else has access to the data, for what purpose and how is security ensured?
6. What are your rights over your data?
7. Who do you contact for concerns about data protection and our privacy policy?

When we talk about processing the data we include the actions of collecting, storing, sharing, analysing, backing up or deleting the data. For clarity we give many illustrative examples and will note explicitly where such examples are not exhaustive.

1. What categories of personal data are collected and processed?

We process your data in order to fulfil our mission as a school.

It is simplest to think in terms of data categories where the processing shares a common purpose. In the table below we list some of the most important data categories for students and parents.

Please note that data for children under 16 are necessarily provided by the parents.

Data category	Examples of typical data
Admissions process	Name, date of birth, previous school details, transcripts, references
Student characteristics	Nationality, language, gender
Student assessment	Teacher reports, homework assignments, external examination results, IB Diploma, SAT if appropriate
Personal identifiers authentication	Unique pupil number, Security badges, security camera records. See section at the end of this document regarding CCTV.
Attendance	Sessions attended, number of absences and reason for absence
Behaviour	Incidents, exclusions
Optional services eg hot lunch	Dietary requirements
Field trips and activities	Passport information (overseas trips)
Medical information	Doctor's report, vaccinations, allergies, individual health plans
Safeguarding	Child protection referral information
Special educational needs	Assessment information, specialist reports

Parent contact information	Email, mobile phone, emergency contact details
Fee payments	Parent's company, occupation, payment details. We may provide your contact details and payments details to a third party payment provider to process the payment.

Please note that this list is not exhaustive and that some categories would apply only to certain students.

We may also collect some additional categories of data if you access our wireless network while visiting one of our campuses or if you browse our website. This information might include your IP address, the name or MAC address of the mobile device you use to connect through, or it might include the exchange of 'cookies' with your device.

Full information is provided at the time of collection of the data.

2. Why is the data collected and how is the data used?

The personal data collected is essential in order for the school to fulfil its stated educational goals as an international school, to meet local legal requirements and to execute the contract between you and the school. We use the personal data we collect for students and parents to:

1. Provide the child with an education
2. Support student learning
3. Engage you as a parent in your child's education
4. Monitor and report on student progress
5. Provide appropriate pastoral care
6. Meet the standards of accrediting authorities
7. Keep children safe
8. Meet the legal requirements placed upon us
9. Ensure the security of the school premises
10. Process payments
11. Process applications to the School

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

For casual visitors to the website we do not collect specific personal data unless you complete a form to contact us or begin the application process. However as with most websites the user's experience is enhanced if cookies are enabled and our website does use Cookies. A notice explaining our policy on cookies appears when you visit our website.

Follow this link to our Cookie policy

3. What is our lawful basis for processing the data?

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing student or parent personal data are that it is necessary:

- To perform or establish a contract (1, 2, 3, 4, 5, 10, 11)
- To comply with a legal obligation (7, 8)
- To protect the vital interests of a data subject (7, 9, 11)

- As part of a task carried out in the public interest (1)
- For the legitimate interests of the controller (6, 9, 10, 11)

One exception to this is where we make use of student personal data in the form of photos, audio or video on the school website, on social media or through other non-private channels. In this case we ask for your explicit consent, giving illustrations of how such data might be used.

Photographs or recordings used for educational purposes

Photographs or media recordings of your child may be taken in the normal course of learning activities at ISP.

Such recordings provide students with useful feedback, help teachers improve teaching practice and are required as evidence of learning for visiting accreditation bodies. Recordings of student presentations must be submitted to the IB as part of the IB Diploma requirements.

You may give consent for the use and for the sharing of such materials through other channels by completing the Media Authorisation form.

Follow this link to the 'Media authorisation form'.

The form also indicates how you can easily withdraw your consent.

In some situations where we collect more sensitive data, we might also ask for consent to share this information in a restricted way. Examples include passport number details for students participating in overseas field trips and individual health plan information for those with medical conditions that need to be known by those caring for them, or for academic reasons with educational administrative bodies. We might for example share details of a particular condition that would entitle a student to extra time in an examination.

4. How the is data collected, stored, for how long and how security is ensured

We collect only the minimum data required for our purposes and keep it only for as long as it is needed to fulfil our contractual and legal obligation.

All personal data we process follows the same data minimisation principle and is:

- Collected lawfully, fairly and transparently
- Collected for the stated specific purposes with no further processing
- Adequate, relevant and limited to what is necessary
- Accurate and up to date (as far as this is possible)
- Retained only for a limited time
- Stored and processed with appropriate security

The majority of data is collected during the application process and in the annual re-registration process. These data include:

- Application and registration forms
- Doctor's form and medical records
- Files from previous schools

The usual means of collection are:

- Through the online application interface
- Through email exchanges
- Via postal services
- During face-to-face meetings

For important information such as emergency contact numbers or active email addresses we work throughout the year to ensure that our records remain accurate and up to date.

We hold student data securely for the set amount of time shown in our data retention schedule.

Where we store some data that may be considered 'high risk' or 'sensitive', we have conducted privacy impact assessments and deployed additional security measures to ensure the data is adequately protected.

For example, sensitive data relating to child protection issues is stored in a system (CPOMS) with additional layers of security. The company providing the system is accredited for both ISO 27001 and UK Government 'Cyber Essentials' which are reviewed each year and their systems and networks are subjected to regular independent penetration testing to ensure the security of the schools' data.

5. Who else has access to the data, for what purpose and how security is ensured

We do not share information about our students and parents with anyone without consent unless the applicable law, the relevant departments within the authorities who have responsibility for education on a statutory basis, or the fulfilment of the contract that is entered for the schooling of a child require us to do so.

For example, we might share some payment details with a third party provider in order to process the payment in application of the contract entered with the School.

We provide portability for any personal data stored in our systems. In the simplest cases this may mean just data exports in standard 'csv' file format or, where it is possible, in a format that allows direct migration to a different system. For example where a student has stored personal work or assignments on ManageBac (our platform for curriculum development, reporting and assessment) these data can, at the request of the parent, be migrated to the child's new school if they also use the ManageBac platform.

We share some core elements of the personal data we keep with vendors who provide information systems or services that are part of our routine operations as a school. For example our online library system (destiny) is run by a company called Follett based in the US.

Where we do so, we enter in agreements with such vendors to ensure they comply with the GDPR's requirement for subcontractors

Where we give students access to these systems through personal accounts we may, depending on the age of the child, also share the account details with parents (children over 16), or ask for them to give their permission for their child(ren) to access the system.

Examples include ManageBac, our online learning platform where students can access curriculum information and homework assignments or Google's education suite where students can store files or collaborate with peers.

Transferring data overseas

We may send your information to other countries in situations where:

- we store information on computer servers based overseas; or
- we communicate with you or your child when you are overseas
  (for example, during the summer holidays if you live in a different country)
- you request that we do so
  (say for a university or job application)

The European Commission has produced a list of countries which have adequate data

protection rules. The list can be found here:

http://ec.europa.eu/justice/data-protection/international- transfers/adequacy/index_en.htm

If the country that we are sending your information to is not on the list or, is not a country within the EEA (which means the European Union, Liechtenstein, Norway and Iceland) then it might not have the same level of protection for personal information as there is in France. For what concerns the subcontractors, we would then require contractually the subcontractor to comply with the GDPR requirements according to GDPR article 28.

Below you will see some examples of our subcontractors with information about how they process personal data. The list is illustrative not exhaustive.

Company	Purpose	Data protection information
Capita	Class attendance lists	SIMS Teacher App
Google	Student email, document storage and collaboration	Google Suite for Education
Faria Systems	Curriculum management, assessment and reporting	Managebac
Follett	Library resources	Destiny Library System

6. What are your rights over your data?

Under GDPR you have the right to:

- Be informed of the personal data we hold on you or your minor children
- Request access to the data without charge
- Have errors rectified
- Request data to be erased; where it is no longer necessary for us to use or keep the information; where you have withdrawn consent or if we have no legal basis to keep the information.
- Restrict further processing of personal data that was shared for a specific purpose
- Request a copy of the personal data we hold in a common digital format such as a csv file (Data portability)
- Compensation for breaches of data protection

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 purpose of direct marketing
- Object to decisions being taken by automated means
- Seek redress, either through the CNIL, or through the courts

7. Who do you contact for concerns about data protection and our privacy policy?

To exercise any of these rights please contact our Data Protection Officer dpo@isparis.edu by email or by post at ISP DPO, 6 rue Beethoven 75016 Paris. Please provide official documentation copy to prove your identity and address together with your request.

We will take all measure to resolve any of your concern regarding our processing of your personal data. However, in cases where despite our efforts have not enable us to resolve your concerns locally, you also have the right to contact the controlling authority, in France the CNIL.

https://www.cnil.fr/en/contact-cnil