International School of Paris

PRIVACY POLICY FOR STAFF

Document Manager: IT Director
Reviewing Committee: School Leadership Team
Last Publication Date: April 2026
Next Review Date: April 2027

Contents

Policy Statement 3
What personal data do we process in relation to our staff? 3
Where do we get personal data from about our staff? 4
Why do we use staff's personal data and on what legal bases? 4
Rights of our staff in relation to their personal data 5
Who can have access to staff personal data? 5
Do we transfer staff's personal data outside of the European Economic Area (EEA)? 5
How long do we keep your data? 5
Concerns 6
Contact Us 6

Policy Statement

We are the International School of Paris ("**We**", "**Us**"). During an individual's employment or engagement with the School, We process, as controller, information relating to them for a range of employment, administrative, legal, and safeguarding purposes.

Information that directly or indirectly identifies an individual is referred to as **personal data**. This includes information provided directly by the individual, as well as information obtained from other people or organisations where appropriate.

Any operation performed on personal data, such as collecting, using, storing, disclosing, or deleting it, is hereafter referred to as **processing.**

This document sets out, in particular, what personal data we process about our staff, why we process that data and the legal bases of the processing, who has access to personal data, how long we process the data, and the rights of individuals in relation to their personal data processed by us.

What personal data do we process in relation to our staff?

We will collect, hold, share or otherwise process the following personal data about our staff:

- **identification data** (such as name, employee or teacher number, French social security number (numéro de sécurité sociale), gender, age, date of birth, nationality, passport details, data relating to the document serving as a work permit, ID photo, family composition and emergency contact details)
- **contact details** (such as address, home and mobile numbers, personal email address)
- **financial details** (such as salary information, bank account details (RIB))
- **professional data** (such as start dates, hours worked, post, roles, type of working contract)
- **work absence information** (such as number of absences and reasons, holiday records)
- **qualifications/training courses attended**, CV information, diploma and, where relevant, subjects taught
- **performance information** (such as appraisals and performance reviews, performance measures including performance management/improvement plans, disciplinary or grievance records)
- **incident information** (such as accident or incident records and reports, disciplinary sanctions, details of injuries, statements given)
- **administrative tracking of employee medical visits** (such as visit dates, fitness for work (fit or unfit)
- **data relating to the management of workplace accident and illness reports/other absences** (such as contact details of the occupational physician, date of the accident or first medical diagnosis of the illness, date of last day of work, date of return to work, reason for absence (work accident or occupational illness))
- **data relating to tools and equipment made available to the employee** (such as log data, computer directories)
- **other information** (such as correspondence using school systems, pension arrangements (AGIRC-ARRCO), time and attendance records, information in applications made for other posts within the school, minutes from meetings, references the school receives or provides to other organisations, supporting documents to prove address and other details, CCTV footage, audio-visual recordings and images)

- **Criminal records data** — as a school working with minors, we are required to verify that staff have not been convicted of offences that would prohibit them from working with children. In accordance with the CNIL's guidance, we ask relevant staff to present their **bulletin numéro 3 du casier judiciaire (B3)** at the time of recruitment. We do not retain a copy of this document. A record of whether the verification was completed ("yes/no") is noted in the employee's HR file.

Where do we get personal data from about our staff?

A lot of the personal data we have about our staff comes from the individuals themselves. However, we may also obtain information from tax and regulatory authorities (including French tax authorities - Direction Générale des Finances Publiques, URSSAF), previous employers, our insurance benefit administrators, consultants and other professionals we may engage, recruitment or vetting agencies, and publicly available resources including online sources. In addition, we may obtain information from our computer networks and systems (including automated back-ups), CCTV and access control systems, remote access systems, email and instant messaging systems, internet facilities, telephones, voicemail and mobile phone records (when mobile phones are provided by ISP).

Why do we use staff's personal data and on what legal bases?

The processing activities described below are carried out by Us on the following legal bases:

- to perform a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- to comply with legal obligations;
- in accordance with our legitimate interests (e.g., to manage IT tools, to manage professional evaluation, to ensure the security of persons and property).

We process the personal data of our staff for the following purposes:

- Recruitment management (e.g., processing applications, managing interviews);
- Administrative management of personnel (e.g., managing employee files, managing internal directories and organizational charts, managing professional elections, provision of employee benefits);
- Management of salary/compensation and completion of administrative formalities (e.g., establishing compensation, nominative social declarations);
- Provision of tools and equipment to staff (e.g., monitoring and maintenance of IT equipment, management of professional email accounts);
- Work organization (e.g., calendar management);
- Career and mobility monitoring (e.g., professional evaluation of staff, management of internal professional skills);
- Training (e.g., management of training requests and completed training periods);
- Management of social assistance;
- Ensuring the security of the persons and property (e.g., management of the video surveillance system);
- Defending against or exercising legal claims and investigating complaints.

Personal data is not used for automated decision-making that produces legal or similarly significant effects on staff without appropriate human oversight.

Rights of our staff in relation to their personal data

All of our staff have the right to request access to personal data that we hold about them.

Individuals also have the right, in certain circumstances, to:

- Object to the processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Restrict processing of their personal data
- Have their personal data erased
- Data portability
- Define guidelines regarding the fate of their data after their death
- Lodge a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL).

To make a request for exercising their rights see the Contact Us section below.

Who can have access to staff personal data?

Personal data about our staff are accessible to:

- Our internal staff, solely for the purposes of their duties and tasks and within the limits of their responsibilities;
- Our service providers acting as processors (e.g., IT service providers);
- Public authorities, where applicable (e.g., French Ministry of Education (Ministère de l'Education Nationale) and the Rectorat de l'Académie de Paris, in compliance with legal obligations, French tax and social security authorities (URSSAF, Direction Générale des Finances Publiques)
- Our professional advisors including legal and HR consultants.

Do we transfer staff's personal data outside of the European Economic Area (EEA)?

Staff's personal data can be transferred to countries outside of EEA. These transfers are either based on European Commission's adequacy decisions or are subject to appropriate safeguards (e.g., Standard Contractual Clauses). You can obtain a copy of these safeguards by sending an email to the address indicated in the Contact Us section below.

How long do we keep your data?

Your personal data is kept only for as long as necessary for the purposes for which it is processed. As a general rule, your data is retained for the duration of your employment contract with ISP. After this period, certain data may be kept for a limited additional time in order to comply with legal and regulatory obligations (in particular for employment, tax or legal purposes), and is then securely deleted or archived.

Concerns

If an individual has any concerns about how we are using their personal data they can contact our **Data Protection Officer.** An individual can also contact the Commission Nationale de l'Informatique et des Libertés (CNIL) should they consider this to be necessary, at https://www.cnil.fr

Contact Us

If you would like to discuss anything in this privacy notice, exercise any of your rights in relation to your personal data, or make a complaint, please contact:

Data Protection Officer
International School of Paris
Email: dpo@isparis.net
Address: 6 rue Beethoven, 75016 Paris, France