

POLICIES AND PROCEDURES

PRIVACY POLICY

Last revision August 2026

1.1 Introduction

ISCS-The British School of Zug is committed to protecting the privacy and security of the personal information of students, staff, parents, prospective employees, and all members of our community. This Privacy Policy explains how we collect, use, share, and protect your personal data in compliance with the applicable laws, such as the Swiss Federal Act on Data Protection of 1 September 2023, and EU data protection regulations (General Data Protection Regulation 2016/679 of 27 April 2016 or GDPR), each as amended or replaced from time to time, and any other relevant legislation.

ISCS acts as data controller through its authorised governing bodies and management. Individual staff members process personal data exclusively in the course of their professional duties and on behalf of ISCS.

1.2 Data collected

We collect various types of personal data (only where strictly necessary for safeguarding, educational support or legal obligations, and is processed with heightened confidentiality), including:

- **Identification Information:** Names, date of birth, gender, nationalities, and copies of identification documents.
- **Contact Information:** Home address, email addresses, phone numbers.
- **Academic and Behavioral Records:** Attendance, grades, report cards, learning support needs, assessments, disciplinary records, and any other necessary academic data.
- **Health and Safety Information:** Medical records (allergies, immunizations, conditions), emergency contact details, accident records, psychological information.
- **Financial Information:** Billing details, bank account information, payment history, and financial assistance records.
- **Employment Information:** For staff and potential candidates, we collect employment history, references, qualifications, certifications, personal, financial information, and background checks.
- **Photographs and videos** (see section 8 below).
- **Relevant correspondence with you**, including, for instance, concerns, particular interests, or how to best communicate with you.
- **Cookies and other website usage data.**

1.3 Purpose of Data Collection and Legal Basis

The School collects and processes data for various purposes, including:

- **Providing Education Services:** To facilitate educational services, maintain academic records, and support students' development.
- **Legal Compliance:** To comply with applicable Swiss laws and regulations, including health and safety requirements.
- **Communication:** To keep students, parents, and staff informed of School activities, events, and updates.
- **Human Resources and Recruitment:** To evaluate, recruit, and manage staff effectively.

- **Security and Safety:** To maintain a safe and secure environment, we may process data relating to health and conduct background checks on employees.
- **Financial Administration:** To process payments, manage billing, and provide assistance where needed.
- **Former students and staff:** To process requests of information of their time at school.

The legal basis for data processing includes the necessity of fulfilling contractual obligations (such as the student's enrollment), compliance with legal requirements, and legitimate interests pursued by the School, especially regarding school safety and operational management. Where processing is based on legitimate interests, ISCS conducts an internal balancing assessment to ensure such interests do not override the rights and freedoms of the data subject.

1.4 How Data is Collected

We collect personal data through various means, including:

- Enrollment forms, contracts, and related documentation submitted by parents and guardians during the admission process.
- Forms and records maintained by teachers and administrative staff, such as academic records, health forms, consent forms, among others.
- Data submitted by job applicants during the recruiting process, including references provided by previous employers.
- Data submitted by employees in the course of their employment.
- Data obtained from authorities, or in the course of administrative or court proceedings.
- Online portals, emails, and communications directly from students, parents, and staff.
- Surveillance systems in school areas to ensure security and safety.
- Data collected through the use of the ISCS website or other online ISCS services (for more information, please refer to the Cookies section below).
- Internal operational records created by staff in the course of educational, pastoral, safeguarding, or administrative duties.

1.5 Sharing of Data

The School takes care to protect your data and only shares it as necessary and as permitted by law:

- **With Service Providers:** To external service providers who assist with services such as IT support, hosting, or recruitment, under strict data protection agreements.
- **With Government Authorities:** Where legally required, such as sharing health information during an outbreak, compliance audits, or student records upon legal request.
- **For Academic and Extracurricular Purposes:** In some cases, data may be shared with educational or extracurricular institutions for purposes like testing or school trips, with prior consent where needed.

Transfers of personal data may occur to countries of the European Economic Area or other countries different from that area and Switzerland. If external organisations are located in countries whose legislation does not guarantee an adequate level of data protection, ISCS will implement suitable safeguards in the form of appropriate contractual clauses and model contracts for data transfers recognised by the Swiss Federal Data Protection and Information Commissioner, in order to ensure compliance with this Policy and applicable laws.

When sharing data with external organisations, ISCS will oblige the external service provider to comply with this Policy and to process personal data securely and exclusively for the purposes allowed to ISCS.

Please be aware that ISCS always signs a contract and/or check with those third parties to have clarity on how they will manage the information provided by the school.

ISCS does not sell, rent or market personal data, and does not transfer personal data to third parties other than set out in this Policy without explicit prior consent or as required under applicable law or regulation.

Data processing by service providers acting as processors under contract does not constitute disclosure to third parties within the meaning of applicable data protection laws.

1.6 Data Security

The School implements robust security measures to protect personal data, including:

- **Technical Measures:** Encryption, firewalls, access controls, and secure storage of data both in physical and digital forms.
- **Organisational Measures:** Access is limited to authorised personnel on a need-to-know basis, with comprehensive training on data protection policies.

In the event of a data breach, the School will promptly assess the impact, notify the affected individuals, and, if necessary, inform relevant data protection authorities following the legal requirements.

In the course of their professional duties, authorised staff members may, where operationally necessary, access or process personal data using devices not owned by ISCS. Such access is subject to internal policies, technical safeguards, and organisational measures designed to ensure confidentiality, integrity, and security of personal data.

ISCS requires that any processing of personal data on non-school-owned devices complies with its internal data protection and information security policies, including access restrictions, password protection, and appropriate handling of data. Detailed rules governing such use are set out in internal staff policies and training materials.

1.7 Personal Data Storage

Data is stored on secure storage spaces, servers, through the use of third-party applications (such as learning applications). It may also be stored in countries of the European Economic Area or others. The access to data is password protected (and 2-way authentication system for the case of the school online platform, Clickedu) and restricted to authorised personnel only. In the case of data stored in countries whose legislation does not guarantee an adequate level of data protection, ISCS implements suitable safeguards in the form of appropriate contractual clauses and model contracts recognised by the Swiss Federal Data Protection and Information Commissioner, in order to ensure compliance with this Policy and applicable laws and regulations. Where personal devices are authorised for work use, automatic cloud synchronisation must comply with ISCS security standards and is subject to internal controls.

1.8 Specific rules regarding surveillance, photographs and videos

To ensure the safety and security of our students, staff, and visitors, ISCS utilises limited video surveillance in designated areas of the campus. Surveillance is implemented strictly for security and safeguarding purposes. Access to recorded footage is restricted to authorised personnel only and is governed by internal procedures. Video footage is stored securely for a limited period, typically not exceeding three (3) weeks, after which it is automatically deleted unless retention is required for specific legal, safeguarding, or security investigations.

Throughout the academic year, photographs and videos may be taken on campus as part of routine educational, operational, or promotional activities. This may include documentation of daily school life, academic projects, events, performances, trips, and student participation in curricular or extracurricular activities. Such images and recordings may be used internally for educational and administrative purposes or externally for school communications and marketing materials (e.g. newsletters, brochures, website, or social media), where appropriate and only in accordance with applicable legal requirements.

Photographs or videos that allow students to be identified are only used externally where the appropriate consent has been obtained from parents or legal guardians, unless another lawful basis applies. Special care is taken when processing images of students with specific health, safeguarding, or special educational needs, and such use is always subject to strict access controls and safeguards.

In the course of their professional duties, authorised staff members may, on an exceptional and strictly limited basis, access or process personal data using devices not owned by ISCS, only where operationally necessary and where no suitable school-owned alternative is reasonably available.

Any such access or processing is subject to ISCS' internal data protection, information security, and acceptable use policies, which define the conditions, limitations, and safeguards applicable to the use of personal devices. In particular, personal data must not be permanently stored on personal devices, must be protected against unauthorised access, and must be transferred to approved school systems without undue delay.

The use of personal devices for the processing of personal data is limited to legitimate educational or operational purposes and is not permitted for informal communication channels or personal messaging applications, unless expressly authorised.

These internal policies are designed to ensure that personal data is processed securely, confidentially, proportionately, and in compliance with applicable data protection legislation.

ISCS requires that personal data processed on non-school-owned devices be adequately protected, including through access restrictions and appropriate technical and organisational measures. Detailed rules governing the use of personal devices, informal communication tools, storage locations, and the handling or deletion of locally stored data are set out in internal staff policies and are addressed through regular training and awareness measures.

For any questions, requests, or concerns relating to surveillance, photographs, videos, or image rights, or to exercise data protection rights, please contact the ISCS Data Protection Office at dpo@iscs-zug.ch.

1.9 Artificial Intelligence and Automated Digital Tools

ISCS may use approved artificial intelligence (AI), generative AI and other automated digital tools for legitimate educational, administrative and operational purposes. Such tools may be used, for example, to support teaching and learning, the preparation of educational materials, administrative tasks, communications, analysis and other school-related activities.

Where the use of AI or automated tools involves the processing of personal data, ISCS applies the same data protection principles and safeguards described throughout this Policy. Personal data may only be processed through AI tools that have been reviewed and approved by ISCS for the relevant purpose. Personal data must not be entered into unapproved AI services or personal AI accounts for School purposes.

Staff must apply the principles of confidentiality, data minimisation and appropriate security when using AI tools. Particular care must be taken when processing sensitive personal data or information

relating to students, including academic, behavioural, finance, personal, health, safeguarding or special educational needs information.

AI and automated tools are intended to support, rather than replace, appropriate professional judgement. Staff remain responsible for reviewing the accuracy, relevance and appropriateness of AI-generated content before it is used for School purposes.

ISCS does not rely solely on AI or automated processing to make significant decisions concerning students, families, employees or applicants where such decisions may materially affect them. Where AI or automated tools are used to support such processes, appropriate human oversight and professional judgement must be maintained.

Where an AI provider processes personal data on behalf of ISCS, it is treated as a data processor or service provider and is subject to the applicable data protection, security and contractual requirements described in this Policy and ISCS' internal data processing inventory and procedures.

1.10 Break Incident Protocol

In the unfortunate event of a data breach:

- We will take immediate steps to contain the breach and assess the extent of any unauthorised access or data loss.
- Affected individuals will be notified within 72 hours if the breach poses a risk to their rights and freedoms.
- Measures will be taken to mitigate the risk of recurrence, including a review of policies and procedures as necessary.

1.11 Data Retention

The School retains personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. Generally:

- **Student and Family Records:** Retained for the duration of enrollment and then archived in accordance with legal requirements. These records are stored in the appropriate school online platform under secure, protected and restricted access, as well as in physical storage space that complies with regulatory requirements.
- **Employee Records:** Retained during the course of employment and for a set period afterwards as required by Swiss employment laws.
- **Health and Safety Records:** Maintained as long as necessary to ensure a safe and compliant environment.

Records are always kept for longer than the relationship between school and family/student/employee in order to defend or exercise claims, meet legal or post-contractual obligations, including legal documentation requirements, and to safeguard other legitimate interests of ISCS. We retain Personal Data after parents, students, staff, service providers / suppliers, volunteers and other persons have left ISCS in order to provide traceability. It is widely accepted that a School should hold data on the achievements and experiences of a child for their benefit in later life should they need to access that information.

1.12 Managing Information of New Potential Candidates

For individuals applying for positions at the School:

- Personal data provided during the application process (e.g., resumes, certifications, references) is used solely for assessing qualifications for the specific role and is stored securely.
- Information on unsuccessful candidates is kept for up to 6 months following the recruitment process, after which it is deleted unless retention is justified by another legal basis or for possible future employment purposes, like having a CV bank of different potential candidates.
- The data is stored securely on secure servers, protected by different level of passwords and access restricted to only authorised personnel.

1.13 Inventory of Processing Activities

ISCS maintains a comprehensive and regularly updated inventory of all personal data processing activities in accordance with applicable data protection regulations, including the Swiss Federal Act on Data Protection and, where applicable, the European General Data Protection Regulation (GDPR). This inventory enables us to document, manage, and review all instances where personal data is collected, stored, shared, and deleted to ensure compliance, transparency, and accountability.

The inventory includes detailed records for each processing activity, including:

- **Data Categories and Subjects:** Identification of the types of personal data processed (e.g., contact details, academic records, health information) and the relevant data subjects (e.g., students, parents, staff, alumni).
- **Purpose of Processing:** Clear documentation of why each category of personal data is collected, stored, or shared (e.g., for admissions, health and safety, or educational support).
- **Legal Basis for Processing:** Specification of the lawful grounds for data processing, such as consent, contractual necessity, compliance with legal obligations, or legitimate interests.
- **Data Retention Periods:** Defined retention schedules that detail how long each data category will be stored before it is deleted or anonymized, aligned with legal requirements and school policy.
- **Data Recipients and Transfer Information:** Identification of any third parties (e.g., IT service providers, external consultants, government authorities) with whom data is shared, along with details on data transfers outside of Switzerland or the European Economic Area, where applicable.
- **Technical and Organisational Security Measures:** Outline of the data protection measures in place to safeguard personal data, such as encryption, access control, and regular security audits.

This inventory not only ensures that ISCS meets its regulatory obligations but also provides a framework for regular assessments and updates to our data protection practices, helping us to maintain data integrity, privacy, and security for our entire school community.

The following table summarises which department is collecting, processing and/or accessing certain data at school, and by which means (school Google Drive, school online platform Clickedu, school hard copy files):

Data collected (who collects, has access and/or processes the data, and by which means). The length and purpose for the data to be retained are outlined in the privacy policy and in the internal data retention policy. Those who appear in the table collect and/or receive the data									
	Admissions	SLT	School Office	Finance	Teachers	Data Processors			
Student's information	Name, Surname	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
	DOB	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
	Gender	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
	Address	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	We don't use this info		
	Place of birth	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	We don't use this info		
	Nationality	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	We don't use this info		
	Number of siblings	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	We don't use this info		
Parents information	Current school	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
	Name, Surname	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
	Phone number	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
	DOB	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
	Nationality	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	We don't use this info		
	Address	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	We don't use this info		
	Occupation	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	We don't use this info		
Student's medical information	Marital status	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	We don't use this info		
	Email	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive	Google Drive		
Student's academic (works produced, exams, grades, progress, behavior, and similar) information	Medical information of student	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	We don't use this info	We don't use this info		
	Progress information about the student	We don't use this info	Clicked Google Drive Hard copy file	Clicked Google Drive Hard copy file	We don't use this info	Google Drive Clicked Hard copy file	We don't use this info		
Photos and videos									
	Data regarding trips, activities	We don't use this info Clicked	Clicked Google Drive	Clicked Google Drive	We don't use this info Clicked	Google Drive Clicked	We don't use this info		

For a better view, it is available under request.

1.14 Cookies and social plug-ins

We use cookies on our website. We use website statistic packages such as Google Analytics to analyse trends in how our website is accessed and utilised. Information monitored includes internet protocol (IP) addresses, geographic location of visitors (country, city), browser type, internet service provider (ISP), referring/exit pages, platform type, date/time stamp, time spent on pages, and keywords used to find our site via search engines. This information is anonymous and cannot be directly linked to individual users. We may use it to identify high-use or low-use areas of the site, pinpoint problem areas of the site, analyse broad demographic trends in our visitors and make decisions about how to make it easier for people to find and navigate our website.

If you do not want Analytics to be used in your browser, you can install the [Google Analytics browser add-on](#). You can set your browser not to accept cookies or to ask each time before storing a cookie. You can also delete cookies on your device by using the corresponding function of your browser. On our Website, you can manage your Cookies preferences at any time.

More information about the ways in which Google Analytics collects and processes personal data can be found here: <https://www.google.com/policies/privacy/partners>.

The social plug-ins used on our Website enable you to recommend and share our content on social media. Social plug-ins used on the Website are labelled with the logo of the respective social network.

Only if you interact with the social plug-in and are logged in to the relevant social network, data will be sent to the respective provider of the social network. This is done using cookies. Please refer to the data protection information of the respective provider.

1.15 Your rights

Individuals have rights concerning their personal data, including:

- **Right to be informed** – be informed of how we are processing your Personal Data – this Privacy Notice serves to explain this to you but do contact us if you have any questions (see Point of Contact details below).
- **Right of Access:** You may request a copy of your data.
- **Right to Rectification:** You may request the correction of inaccurate or incomplete data.
- **Right to Erasure:** You may request the deletion of your data in specific circumstances.

- **Right to Restrict Processing:** Under certain conditions, you may request the restriction of processing.
- **Right to data portability** – allows you to receive Personal Data that you have provided us in a structured, commonly used machine readable format. It also allows you the right to request us to transmit this data to another controller.
- **Right to Object:** You may object to data processing based on legitimate interests or direct marketing.
- **Right to withdraw consent** – in those instances in which the processing of your Personal Data is based on consent, you have the right (subject to age provisions) to withdraw that consent. Please note that the processing will end from the moment the withdrawal takes place without any effect on the processing that took place prior such withdrawal.
- **Right to complain** – while the first point of contact related to the processing of your Personal Data or in exercising any of the rights identified above should be us (see Point of Contact below), you also have the right to directly contact the Supervisory Authority in Switzerland:

Federal Data Protection and Information Commissioner (FDPIC)

Feldegweg 1
CH- 3003 Berne
Switzerland

There may be instances where you may not want us to process or share your Personal Data. In these cases, we may not be able to fulfil the service you need, or do so in a limited way, or be able to comply with a statutory obligation. In those instances, we will not be able to comply with your request and we will tell you if that is the case.

ISCS responds to requests relating to the processing of Personal Data in accordance with applicable data protection legislation and, in principle, within one (1) month of receipt. Where a request is particularly complex, extensive, or involves a high volume of data, this period may be extended in accordance with the law. In such cases, ISCS will inform the requesting party of the extension and the reasons for it within the initial response period. In responding to any request, ISCS will always ensure that the rights and freedoms of third parties are protected, which may require the redaction or restriction of certain information. Where appropriate, and in compliance with legal requirements, ISCS may also offer the possibility of an on-site review of relevant records as an alternative or complement to the provision of copies.

For any requests or questions regarding your data rights, please contact us at dpo@iscs-zug.ch.

1.16 Changes to This Privacy Policy

This Privacy Policy is subject to periodic review and may be updated to reflect changes in legislation or School policies. We will notify you of any significant changes by posting updates on our website and through email notifications where appropriate.

1.17 Contact us

For questions or concerns regarding this Privacy Policy or any data protection matter, please contact:

Data Protection Office: dpo@iscs-zug.ch