POLICIES AND PROCEDURES

ISCS SCHOOL DATA RETENTION POLICY

1. Purpose

This Data Retention Policy establishes how ISCS International School of Central Switzerland collects, stores, retains, and deletes personal data of students, parents, guardians, and staff in compliance with the Federal Act on Data Protection (FADP). The objective is to ensure lawful, transparent, and proportionate handling of personal data within the school environment. This policy also aligns with the General Data Protection Regulation (GDPR) where applicable, as ISCS processes data of EU citizens.

2. Scope

This policy applies to:

- All personal data processed by ISCS International School of Central Switzerland, regardless of the form (digital or paper).
- All staff members, contractors, and service providers handling personal data on behalf of the school. It also covers personal data stored with third-party providers such as Google Workspace for Education and Clickedu, subject to contractual safeguards.

3. Principles

In accordance with the FADP, the school adheres to the following principles:

- **Lawfulness & Transparency**: Personal data is processed lawfully, fairly, and transparently.
- **Purpose Limitation**: Data is collected for specific educational, administrative, or legal purposes only.
- **Data Minimisation**: Only the data necessary for these purposes is processed.
- **Accuracy**: Data is kept accurate and up to date.
- **Storage Limitation**: Data is retained only as long as necessary for the defined purpose or legal requirements.
- **Security**: Appropriate technical and organisational measures are in place to protect personal data.

4. Data categories and retention periods

The following retention periods apply unless specific cantonal or federal legislation requires longer or shorter retention:

- **Student Records (enrolment, grades, reports, diplomas)**: Retained for 10 years after the student leaves the school.
- **Health and Special Needs Data**: Retained only as long as necessary for student welfare, then securely deleted (maximum 2 years after student leaves, unless legal obligation applies).
- **Attendance Records and Disciplinary Actions**: Retained for 5 years after the student leaves.
- **Financial Data (invoices, tuition fees, grants)**: Retained for 10 years in accordance with Swiss accounting law.
- **Staff Records (employment contracts, performance reviews, payroll)**: Retained for 10 years after the end of employment, unless longer required for pension or tax purposes.
- **Access Logs and IT System Data**: Retained for a maximum of 12 months, unless required for security or investigation.

5. Secure deletion

At the end of the retention period, personal data must be securely deleted or anonymised. Secure deletion methods include:

- Shredding of paper records.
- Irreversible digital deletion.
- Anonymisation where ongoing use for statistics is justified. ISCS also ensures that contracted third-party providers apply equivalent secure deletion measures in accordance with their data protection agreements.

6. Responsibilities

- **School Board / Management**: Ensures compliance with this policy.
- **Staff Members**: Must adhere to this policy in their daily work.

7. Rights of data subjects

Students, parents, guardians, and staff have the right to:

- Request access to their personal data.
- Request rectification of inaccurate data.
- Request deletion of data where no legal obligation prevents it.
- Object to processing in justified cases.

Requests will be handled in accordance with the FADP and must be addressed to the school's designated contact person for data protection. As minors, student rights are typically exercised by their parents or guardians, though students acquire increased rights as they mature.

In addition, other rights such as the right to restrict processing, the right to data portability, the right to withdraw consent, and the right to lodge a complaint with the Federal Data Protection and Information Commissioner (FDPIC) are set out in the ISCS Privacy Policy.

8. Review of policy

This policy will be reviewed at least every two years, or earlier if required by changes in legislation, cantonal requirements, or operational needs.

Adopted by: ISCS International School of Central Switzerland

Date: 1st of September 2025

Next Review Date: 1st of September 2027

You can access log events data and reports data this far back:

Log events data or report name	Data retention time
Access Transparency log events data	6 months
Account activity reports	6 months
Admin log events data	6 months
Admin Data Action log events data	6 months
Assignments log events data	6 months
Audit data retrieved using the API	6 months
Calendar log events data	6 months
Chat log events data	6 months
Chrome apps and extension usage report	12 months
Chrome log events data	6 months
Chrome version report	12 months
Classroom log events data	6 months
Cloud Search log events data	6 months
Context-aware access log events data	6 months
Data migration log events data	6 months
Customer/User usage data retrieved using the API	15 months
Devices log events data (availability of these logs depends on your subscription)	6 months
Drive log events data	6 months
Email log search	30 days
Entities usage data retrieved using the API	30 days
Gemini for Workspace log events	6 months
Gmail log events	6 months
Google Workspace Quota log events	6 months
Groups log events data	6 months
Keep log events data	6 months
Looker Studio log events data	6 months

Meet hardware log events data	6 months
Meet log events data	6 months
Meet quality tool	30 days (Meetings older than 28 days are not displayed in the Admin Console)
OAuth Token log events data	6 months
Rules log events data	6 months
SAML log events data	6 months
Secure LDAP log events data	6 months
Security reports	6 months
Tasks log events data	6 months
Users	6 months
User log events data (previously named Login audit log)	6 months
Vault log events	Indefinite
Voice log events data	6 months