SAPIENS INNOVATIVE SCHOOL
Data Protection (GDPR) Policy

1. Purpose

This policy outlines how Sapiens Innovative School collects, processes, stores, and protects personal data of students, parents, employees, and partners in accordance with the **General Data Protection Regulation (GDPR)** and relevant **Polish law (Ustawa o ochronie danych osobowych)**. Our goal is to ensure transparency, safety, and respect for the privacy of all members of our school community.

2. Legal Framework

This policy is based on:

- **RODO (Rozporządzenie o Ochronie Danych Osobowych) – EU GDPR**
- **Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000)**
- **Recommendations from UODO (Polish Personal Data Protection Office)**
- **Cambridge International's expectations for secure data practices**

3. Definitions

Personal data: any information relating to an identified or identifiable person (e.g., name, email, ID number, health data, academic performance).

Data subject: any individual whose data is processed (students, parents, employees, etc.).

Processing: any operation on personal data (collection, storage, use, transfer, deletion).

Data Controller: Sapiens Innovative School, which determines the purposes and means of processing personal data.

Data Processor: a third party (e.g., IT provider) that processes personal data on behalf of the school.

4. Guiding Principles

The school ensures all data is:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Stored only as long as necessary
- Processed securely and confidentially

5. Roles and Responsibilities

School Leadership and Administration

- Acts as Data Controller
- Ensures legal compliance and data protection awareness
- Appoints a Data Protection Officer (DPO) if legally required

Teachers and Tutors

- Handle data in accordance with this policy
- Complete GDPR training as required
- Report data breaches or concerns immediately

Students and Parents

- Have the right to access, correct, and delete personal data
- Are informed about their data rights during enrollment

6. Lawful Basis for Processing

We process personal data based on:

- **Legal obligation** (e.g., educational records, health reporting)
- **Contractual necessity** (e.g., enrollment contracts)
- **Legitimate interest** (e.g., school communication)
- **Consent** (e.g., use of student photos for promotion)
- **Vital interests** (e.g., in medical emergencies)

7. Data Collection and Use

We collect data such as:

- **Student data**: name, age, contact details, academic records, health and SEN information
- **Parent/guardian data**: contact information, billing data
- **Employee data**: contracts, ID, payroll, background checks

This data is used for:

- Educational and administrative purposes
- Health and safety management
- Legal reporting (e.g., to MEN, Kuratorium, Sanepid)
- Communication with families
- Promoting school events (with consent)

8. Data Security and Storage

- Data is stored securely on password-protected systems (e.g., School Today, encrypted drives)
- Paper records are locked in secure cabinets
- Access to sensitive data is restricted to authorised personnel
- Regular data backups and IT security protocols are in place

9. Data Sharing and Transfers

We may share data with:

- Educational authorities (e.g., Kuratorium, MEN)
- Health or emergency services
- Technology providers (e.g., Librus, School Today) under data processing agreements
- External exam bodies (e.g., Cambridge Assessment)

We do **not** transfer personal data outside the EEA unless adequate protection measures are in place.

10. Rights of Data Subjects

Individuals have the right to:

- Access their data
- Rectify inaccurate or incomplete data
- Request data deletion ("right to be forgotten")
- Restrict or object to processing
- Data portability (where applicable)
- Lodge a complaint with **UODO** (https://uodo.gov.pl)

11. Consent Management

- Parental consent is required for data use not covered by legal or contractual obligations (e.g., image use)
- Consent can be withdrawn at any time
- Consent forms are updated annually or as needed

12. Data Breach Response

- All breaches must be reported to the Headmaster or designated officer within 24 hours
- Major breaches are reported to UODO within 72 hours as required by law
- Affected individuals will be notified when there is a high risk to their rights

13. Data Retention

Data is retained as follows:

- Student records: up to 5 years after graduation
- Financial records: minimum 5 years
- Staff employment records: 10 years after end of employment
- Health and safety / incident records: according to legal requirements

14. Monitoring and Review

This policy is reviewed annually or earlier if required by law. Input from staff and families is encouraged to ensure data protection remains strong and relevant.

Approved by
Olena TkachovaHeadmaster
Date: 06.08.2025