

POLICY ON PERSONAL DATA PROCESSING

Last Update: January 2026

Cambridge School of Bucharest, operated by **Fundația Mateas**, is committed to protecting the personal data of students, parents/guardians, staff and all individuals who interact with the School.

This Policy explains how we process personal data, the legal bases for such processing, the digital platforms we use (including AI-based tools), and the rights of data subjects under the General Data Protection Regulation (EU) 2016/679 (“GDPR”).

1. WHO WE ARE

Fundația Mateas

126C Erou Iancu Nicolae Street, Voluntari, Ilfov, Romania

Registered under no. 8PJ/02.02.2022 in the Register of Associations and Foundations

CIF: 3580797

The School acts as **personal data controller** for all processing activities described in this Policy.

For certain services (such as catering and transport), the School acts as a **joint controller** together with **GRANOR SRL**.

2. DATA PROTECTION OFFICER (DPO)

The School has appointed **Battlegroup SRL** as its external Data Protection Officer (DPO).

You may contact the DPO for any matter relating to this Policy:

DPO: Battlegroup SRL

Email: dpo@battlegroup.ro

Website: www.battlegroup.ro

3. WHAT PERSONAL DATA WE PROCESS

We process personal data belonging mainly to two categories:

- (a)** School employees and collaborators, and
- (b)** Students and their parents/legal guardians.

A. Data processed about employees and collaborators

As required for employment and HR administration:

- identification data (name, surname, CNP, ID/passport details, address, signature)
- contact data (phone, email)
- emergency contact details (name, relationship, phone number), provided voluntarily for health and safety purposes
- copies of ID and civil status documents

- diplomas and qualification documents
- bank account data
- criminal record certificate (where legally required)
- health data related to workplace safety and employment law

B. Data processed about students and their parents/guardians

We process:

- name and surname
- date of birth, sex, nationality
- CNP (where legally required), ID/passport details
- address, contact details
- previous education records
- academic data (grades, assessments, reports, learning progress, behaviour)
- platform-generated data (Engage, Microsoft 365/Teams, Tapestry, Mindjoy, Canva for Education, Copilot and other approved EdTech tools)
- IT usage data (login credentials, device identifiers, security logs, monitored internet access for safeguarding and safety)
- image and voice recordings for promotional purposes, processed only based on explicit parental consent
- health and wellbeing data (accidents, allergies, immunisations, counselling, safeguarding information)

We do not process biometric data for the purpose of uniquely identifying individuals. The School uses educational platforms that may involve limited forms of automated analysis or profiling, such as learning progress tracking, engagement metrics, or adaptive learning features. These activities are used solely to support teaching and learning and do not produce legal or similarly significant effects on students, nor are decisions taken solely through automated processing within the meaning of Article 22 GDPR.

4. PRINCIPLES OF DATA PROCESSING

In accordance with GDPR, all personal data processed by the School is:

- processed lawfully, fairly and transparently
- collected for specified and legitimate purposes
- adequate and limited to what is necessary
- accurate and kept up to date
- stored for no longer than necessary
- processed securely to ensure confidentiality, integrity and availability

5. PURPOSES AND LEGAL BASES OF PROCESSING

A. Contractual necessity – Art. 6(1)(b) GDPR

We process personal data when necessary to enter into and perform the educational contract, including:

- delivering educational services and managing the student's academic record;
- organising examinations and assessments;
- communicating with parents/guardians regarding academic progress, attendance, wellbeing or administrative matters;
- providing access to educational platforms, digital tools, online learning environments, and other systems required for the delivery of education;
- managing extracurricular activities and School-related services agreed in the tuition contract.

B. Compliance with our legal obligations – Art. 6(1)(c) GDPR

We process personal data where necessary to comply with Romanian legal requirements, including:

- education regulations and mandatory reporting;
- health and safety obligations applicable to schools;
- regulations relating to child protection and safeguarding;
- accounting, tax and financial reporting obligations;
- obligations derived from labour law (for staff data).

C. Legitimate interests of the data controller – Art. 6(1)(f) GDPR

We process personal data where it is necessary for the legitimate interests of the School, provided that such interests do not override the rights and freedoms of students or parents. These include:

- ensuring safety and safeguarding within the School campus;
- operating **video surveillance (CCTV)** in designated common areas and external perimeters to protect students, staff and property;
- ensuring the integrity, fairness and proper conduct of examinations, including, where necessary, through limited audio-video recordings using the School's existing **CCTV system during exam sessions**;
- preventing, detecting and investigating misconduct or security incidents;
- monitoring IT systems to ensure security, prevent misuse and support operational continuity;
- administrative management and improvement of educational and support services.

Our legitimate interests never override the rights and freedoms of students, especially minors, all such processing being subject to a prior internal legitimate interest assessment.

D. Consent – Art. 6(1)(a) GDPR

The School relies on **explicit parental consent** for certain processing activities, including:

- the use of student **images, video, audio recordings, or achievements** for communication or promotional purposes;
- publishing content on external platforms such as Meta (Facebook, Instagram), X, LinkedIn, YouTube or similar services;
- the use of optional **AI-based educational tools or features** that are not strictly necessary for the delivery of the educational contract and that involve the processing of student personal data;
- participation in optional programmes, activities or events not required by the educational contract.

Consent is voluntary and may be withdrawn at any time without affecting the student’s right to education or producing any other negative effects.

E. Special category data – Art. 9 GDPR

The School processes special category data (e.g., health, wellbeing, counselling information) only when necessary and based on one of the following legal grounds:

- **Art. 9(2)(h) GDPR** – provision of healthcare, counselling or wellbeing services;
- **Art. 9(2)(g) GDPR** – substantial public interest as recognised under Romanian law, including safeguarding of minors;
- **Art. 9(2)(c) GDPR** – protecting vital interests of the student or another individual where the data subject is unable to give consent.

Where counselling or wellbeing support is not covered by a legal obligation or by the need of protecting vital interests of the student or another individual where the data subject is unable to give consent under Article 9(2)(c) GDPR, or by the provision of healthcare, counselling or wellbeing services under Article 9(2)(h) GDPR the School obtains explicit parental consent in accordance with Article 9(2)(a) GDPR.

6. DIGITAL PLATFORMS, IT MONITORING & AI TOOLS

The School uses digital systems approved for educational and administrative purposes, including:

- Microsoft 365 (Outlook, Teams, OneDrive, Copilot for Education)
- Engage
- Tapestry
- Mindjoy
- Canva for Education
- Other approved EdTech and AI tools

Use of AI Educational Tools

The use of AI-based educational tools that are strictly necessary for the delivery of the educational contract is based on contractual necessity under Article 6(1)(b) GDPR. Explicit written parental consent is required only for optional AI-based tools or features that are not necessary for the delivery of the educational contract and that involve the processing of student personal data.

As a rule, no special category data is entered into AI systems. Any exception would require a documented assessment, an appropriate legal basis, and the use of approved tools with adequate safeguards.

Video Surveillance and Examination Monitoring

The School uses video surveillance (CCTV) in designated areas of the campus for safety, security, and safeguarding purposes. CCTV cameras are placed only in common areas and external perimeters; no surveillance takes place in bathrooms, changing rooms or other sensitive spaces. Recordings are retained for a limited period of maximum **20 days**, in accordance with legal and operational requirements, and are accessible only to authorised personnel.

For certain official examinations or assessments, the School may use audio-video recording inside classrooms to ensure the integrity, fairness, and proper conduct of the examination process. Such recordings are strictly limited to the duration of the exam, are accessed only by authorised staff, and are deleted after the required retention period. These recordings are not used for student evaluation beyond misconduct verification and are not shared with external parties unless legally required.

In certain cases, additional devices (such as webcams or laptops) may be temporarily used to allow authorised external examiners or official bodies to observe examination sessions remotely. Such access is limited to the examination duration and subject to appropriate access controls.

Online admission examinations are supervised via live webcam access solely for invigilation purposes and are not recorded.

Audio-video recordings are reviewed exclusively by authorised staff for human assessment purposes. The School does not use AI systems to analyse behaviour, detect cheating, or make automated determinations based on such recordings.

IT Monitoring

For security and safeguarding, the School monitors:

- login and platform access
- internet usage
- device activity within the School network

This monitoring is proportionate and does not involve profiling or automated decision-making.

7. SOCIAL MEDIA AND AI MODEL TRAINING

When parents consent to the publication of student images, videos or other content, they acknowledge that:

- social media platforms such as **Meta (Facebook, Instagram), X (formerly Twitter), LinkedIn, YouTube** and others may **further process** that content
- such further processing may include **analytics, algorithm optimisation, or AI model training**, according to the platform's Terms of Service
- such processing may involve **transfers of personal data outside the EU/EEA**, including to service providers located in the United States, in accordance with the platforms' own data protection frameworks.
- the School cannot control how these platforms use publicly uploaded content

The School will **never** publish student-related content without explicit parental consent.

8. COLLABORATION WITH UNIVERSITIES (FOR HIGH SCHOOL STUDENTS ONLY)

When universities request contact information for academic presentations or orientation activities, the School may share a student's **School email address** only when:

1. the student voluntarily provides it; **and**
2. for students under 18, the parent/guardian gives **explicit written consent**.

Students aged 18 and over may consent independently.

9. DISCLOSURE OF PERSONAL DATA

We may disclose data to:

- IT and EdTech service providers
- GRANOR SRL (for catering and transport services)
- healthcare or counselling professionals
- supervisory or public authorities where required by law

Where required, personal data transfers are governed by data protection agreements concluded in accordance with Article 26 or Article 28 GDPR, as applicable.

International Data Transfers

Where data is transferred outside the EU/EEA for the sole purpose of fulfilling our contractual obligations, we apply:

- Standard Contractual Clauses
- Adequacy decisions
- Additional safeguards (encryption, access controls)

10. RETENTION PERIODS

Personal data is stored only as long as necessary to fulfil the purposes for which it was collected.

Examples:

- education records: duration of schooling + statutory archiving periods
- billing and accounting: according to fiscal law
- IT logs: according to internal security policies
- counselling and safeguarding records: according to professional/legal standards
- images/media: until parental consent is withdrawn

11. RIGHTS OF DATA SUBJECTS

Students (depending on age) and parents/guardians may exercise the right to:

- access their personal data
- rectify inaccurate data
- request deletion or restriction of processing
- object to certain processing activities
- data portability (where applicable)
- withdraw consent
- lodge a complaint with the Romanian Data Protection Authority (ANSPDCP)

Requests may be addressed to:

- the **Admissions Team**, or
- the **Data Protection Officer (DPO)** at dpo@battlegroup.ro

Proof of identity may be required.

12. LEGAL REQUESTS

We access, retain or disclose information:

- in response to legal requests where required by law
- when necessary to detect, prevent or respond to fraud, misuse, safety threats or violations of School policies
- when required for safeguarding and protection of students
- where otherwise permitted or required under applicable law

13. SECURITY MEASURES

The School applies technical and organisational measures to protect personal data from:

- unauthorised access
- misuse or disclosure
- alteration
- accidental loss or destruction

All employees and third parties acting on behalf of the School must maintain confidentiality and comply with GDPR and this Policy.

14. UPDATING THIS POLICY

This Policy may be updated periodically; thus, you are kindly asked to review the updated version regularly.

The date of the most recent update will be shown at the top of the document.