Personal Data Protection Policy

Review Frequency: Annual
The policy was written by: Legal Division, October 2019
Last reviewed by: Legal Division/School Administration Team/Personal Data Protection Officer
Last review date: November 2024

Sophio Bazadze
Director

GEORGIA "EUROPEAN SCHOOL" Ltd 205172917

2 I. Skhirtladze Str. Tbilisi, 0177, Georgia
Tel: (032) 239 59 64,
info@europeanschool.ge
www.europeanschool.ge
ს/კ: 205172917

Contents

Preamble

The Personal Data Protection Policy (hereinafter referred to as the "Policy") outlines the procedures and requirements for the processing of personal data by "European School" LLC (hereinafter referred to as the "School").

The purpose of this Policy is to ensure that the personal data of the school community is processed in compliance with legal requirements, while protecting it from unlawful or unauthorized use, accidental loss, or damage.

The management of the School is responsible for presenting this Policy and any amendments to the school community, addressing their feedback, and, if necessary, organizing relevant working meetings with school staff.

This Policy governs access to personal data processed by the School, including data stored within the School or on its electronic devices, by any individual (students, their legal representatives, school staff, or other employed persons). School staff, students, parents/legal representatives, and school contractors are required to adhere to this Policy. Non-compliance with the requirements of the Policy will render the school management accountable.

Article 1. Scope

This Policy governs the processing of personal data belonging to school personnel, pupils, students, their parents/legal representatives, and other natural persons connected to the European School. The processing may be carried out through automatic, semi-automatic, or non-automatic means.

Article 2. Definition of Terms

The terms used in this Policy shall have the meanings as defined by the Law of Georgia on "Personal Data Protection."

Article 3. Principles and Basis of Personal Data Processing

When processing personal data, the following principles must be observed, and a legitimate basis for data processing must exist:

1. First Principle: Personal data must be processed fairly, lawfully, transparently, and without compromising the dignity of the data subject.

1.1. The School's legal acts define or should define the data processing procedures, the purpose of each processing activity, the types of personal data being processed, and the legal basis for processing. The legal basis for processing personal data may arise from the following:

- The data subject voluntarily consents to the processing of their personal data for one or more specific purposes.
- Personal data processing is necessary for the signing or execution of an agreement with the data subject and for reviewing their applications (e.g., providing services, monitoring personnel activities, conducting annual assessments, signing agreements with staff or students, etc.).
- Data processing is required by law.
- Data processing is necessary for the School to fulfill its obligations under Georgian legislation.
- The processing of personal data is essential to protect the vital interests (life or health) of the data subject (e.g., providing emergency medical services).
- Processing is necessary to protect significant public interests in accordance with the law.
- Processing is required to protect the legitimate interests of the School or third parties, except when the interests of the data subject's rights and freedoms outweigh such legitimate interests (e.g., the School's legitimate interests are not overridden by the data subject's rights).
- The data is publicly available under the law or has been made available by the data subject.

1.2. The processing of special categories of data is permitted only with the written consent of the data subject or in the following cases:

A) The processing of data related to criminal records and health status is necessary due to the nature of labor obligations and relations, including for making employment decisions.

B) The processing of data is required to protect the vital interests of the data subject or a third party, and the data subject is physically or legally incapable of consenting to the data processing.

C) The data is processed by the European School or public health authorities to protect the health of an individual, as well as when necessary for the management or functioning of the healthcare system.

D) The data subject has made the data publicly available without explicitly prohibiting its use.

E) The data is processed to support the right to education for persons with special educational needs.

F) In other cases provided for by the legislation of Georgia.

Manual

Authorized personnel must accurately and comprehensively explain to the data subject the legal basis for processing their personal data, the purpose of the processing, and provide complete information

about the data processing activities. Consent refers to the data subject's expressed will to allow the processing of their personal data for a specified purpose, given orally, via telecommunication, or through other appropriate means after receiving relevant information.

Authorized personnel handling personal data are obligated to ensure that the data subject has consented to the processing of their personal data. Data subjects must also be informed of their right to refuse consent and their right to withdraw consent at any time, ceasing further data processing.

This Policy includes consent forms for personal data processing, which are provided to learners (Appendix 1) and European School staff (Appendix 2).

Minors have a unique right to the protection of their personal data, as they may not fully understand the risks, consequences, protective measures, and rights associated with data processing. Therefore, personal data of minors can only be processed with the consent of their parent or legal representative.

The processing of personal data must remain transparent to the data subject. All information and communication regarding data processing must be easily accessible, understandable, and presented in clear, simple language. Data subjects must be informed about the rules of data processing, associated risks, protection measures, and their rights.

When personal data is transferred to authorized school personnel by the data subject, the date of receipt of the data must be recorded. If the school obtains personal data independently of the data subject, the data must be stored for a reasonable period of time.

School admissions and enrollment services are required to collect only the information (documents) necessary for fulfilling their functions. This includes personal data related to pupils and their parents/legal representatives.

The human resources management service may request information (documents) that include personal data of European School staff or candidates, as necessary for executing employment contracts and managing labor relations within the framework of the European School's policies.

The Office of University Education and Career Planning should request only the information (documents) necessary to fulfill its functions. This includes personal data related to the student and their parents/legal representatives.

2. The Second Principle: Restriction on the Processing of Personal Data - Personal data may only be processed for specific, clearly defined, and lawful purposes. Further processing of data for purposes that are incompatible with the original purpose ("limitation of purpose") is prohibited. Data processing must align with the stated purposes and be limited to what is necessary to achieve those goals.

Further processing of personal data for purposes incompatible with the original purpose is prohibited. To determine whether further processing is consistent with the original purpose of data collection, the school must, after fulfilling all initial processing requirements, take the following into consideration:

- Evaluate the relationship between the initially collected personal data and the purpose of the further data processing, particularly if it involves special categories of data.
- Assess the context in which the personal data was initially collected and reasonably determine whether the data subject would likely consent to further processing of the data.
- Examine the potential consequences of the further processing of personal data for the data subject.
- Ensure the availability of appropriate protection measures between the initial processing and subsequent processing activities.

3. The Third Principle: Adequacy and Relevance in Data Processing

The processing of personal data must be adequate and relevant to the purpose for which it is being processed, and should only extend to the extent necessary to achieve the legitimate purpose ("Minimizing Data Processing").

Data must be processed only to the degree required to fulfill the relevant lawful purpose. The data must be adequate and proportionate to the goal for which it is processed.

Manual

The scope of personal data processing must align with achieving a legitimate purpose. Processing data that is unrelated or inappropriate to the intended purpose is strictly prohibited.

4. Fourth Principle: Veracity and Accuracy of Data ("Accuracy")

Personal data must be truthful, accurate, and updated as necessary. Data collected without a legal basis or inconsistent with the purpose of processing must be blocked, deleted, or destroyed.

Manual

Authorized personnel must ensure that the data is current and complete, as incomplete or outdated information may result in incorrect data processing. In some cases, it may be necessary to notify the data subject that incomplete or inaccurate data has been corrected.

5. Fifth Principle: Data Retention Period

Personal data can only be stored for the duration and extent necessary to achieve the purpose of data processing. Once the purpose of data processing has been achieved, the data must be blocked, deleted, destroyed, or stored in a form that no longer identifies the individual, unless otherwise stipulated by law.

Manual

Authorized personnel must inform the data subject of the storage period as prescribed by Georgian legislation. If the law does not specify a storage period, the duration should be minimal and determined by the school. To prevent unauthorized retention of personal data, the authorized personnel must establish a final period after which the data will be blocked, deleted, destroyed, or stored in a form that does not identify the individual.

6. Sixth Principle: Data Security and Confidentiality

Data processing must be conducted in a manner that ensures the security of data and protects it from unauthorized or illegal use.

Manual

Data security refers to the ability of a network or information system to withstand accidents, illegal activities, or harmful actions that compromise the access, authenticity, integrity, or confidentiality of transmitted or archived data.

- Authorized personnel must implement organizational and technical measures to safeguard data against accidental or illegal destruction, alteration, disclosure, extraction, or any other form of illegal use or accidental loss.
- The measures taken to ensure data security must be proportionate to the risks associated with data processing.
- Authorized personnel and any employee of the European School involved in data processing must act within the scope of their authority. They are also obligated to maintain the confidentiality of data, including after their official duties or employment have ended.

7. Seventh Principle: Accountability

The school and the individuals authorized to process personal data are responsible for ensuring that the school's personal data protection policy complies with the current legislation of Georgia.

Manual

- The responsibilities and functions of authorized personnel involved in personal data processing must be defined through an order, contract, or other legal document issued by the school director.
- School teachers, members of the supervisory board, and all employees must undergo appropriate training to understand and comply with the requirements of personal data protection laws.
- The school's legal acts must designate a person responsible for supervising the legality of personal data processing. This individual will oversee compliance with the legislation on personal data protection.

Article 4. Special Categories of Personal Data

1. The processing of special categories of personal data is permitted only if the school ensures the protection of the rights and interests of the data subject, and one of the following grounds is met:

A) The data subject has provided written consent for the processing of special categories of personal data for one or more specific purposes.

B) The processing of special categories of data is explicitly and specifically regulated by law and constitutes a necessary and proportionate measure in a democratic society.

C) The processing of special categories of data is essential to protect the vital interests of the data subject or another person, and the data subject is physically or legally unable to provide consent.

D) The processing of special categories of data is necessary in the context of social security and social protection, including managing social security systems and services, to fulfill obligations imposed on the school by Georgian legislation or to exercise specific rights of the data subject.

E) The processing of special categories of data is required due to the nature of labor obligations and relations, including for making employment decisions or assessing an employee's labor skills.

F) The data subject has made their data public without imposing an explicit prohibition on its use.

G) The processing of special categories of data is necessary to protect important public interests.

H) The processing of special categories of data is conducted to support the right to education for persons with disabilities and individuals with special educational needs.

I) The data is processed for other purposes as specified under Article 6 of the Law of Georgia "On Personal Data Protection."

In all cases where data is processed under this Article, the disclosure of data to third parties or the public without the explicit consent of the data subject is strictly prohibited.

Article 5. Data Subject Rights

The data subject has the following rights regarding the processing of their personal data:

A) To receive from the school the following information about the processing of their personal data:

- Details of the individual authorized by the school to process personal data.
- The purpose and legal basis for data processing.
- Whether providing data is mandatory or voluntary; if mandatory, the legal consequences of refusing to provide the data.
- The data subject's right to:
    - Receive information about the data being processed.
    - Request correction, updating, addition, blocking, deletion, or destruction of the data.
- Information regarding the transfer of data to third parties.
- Additional details on the further use of the processed data.
- Specification of the scope of data processing.

B) To withdraw their consent for data processing and request the termination of data processing and/or the destruction of processed data.

C) To request the update or correction of inaccurate or incomplete data.

D) To request the deletion or destruction of data. This right is subject to limitations and will be exercised in compliance with the requirements of applicable legislation.

E) To file a complaint or application with the Personal Data Protection Service or the court. The data subject also has the right to request that the body reviewing the case block the data until a decision is made.

F) To request the termination of data processing. This right is also subject to limitations and will be enforced in accordance with applicable legislation.

Article 6. Online Learning / Learning and Work Process

Photographs and/or videos taken during the online learning process, as well as remote meetings, constitute personal information of individuals. It is strictly prohibited to take photos and/or videos during these processes and to distribute such materials (including for humorous purposes) via any means, including but not limited to social networks. This regulation aims to protect individuals from bullying, unwanted exposure, and the illegal dissemination of personal data.

Article 7. Photography, Digital Images, and Their Publication

Photography and the use of digital devices to record school activities are integral aspects of school community life. During participation in school activities, individuals associated with the school may use photographic (analog/digital) and recording (analog/digital) devices. The purpose of utilizing personal data in these formats is to communicate with the school community.

Permissible Uses of Photographs or Recordings:

- Capturing images of employees participating in school activities.
- Incorporating images in teaching materials or publishing them in digital or analog formats on internal digital tablets or presentation/message boards.
- Monitoring and inspecting school personnel.
- Recording photo, video, or audio content of school events, such as training sessions, recruitment activities, open days, and symposia.
- Documenting school achievements and public events through digital recordings (photo, video, audio) for publication on the school's website and other social media platforms (e.g., Facebook, Instagram, Twitter).
- Recording photo, video, or audio content of any activity or event organized by the school.

The data subject must be aware that any event organized by the school may involve digital image, photo, video, or audio recording.

School staff must be informed about the school's child protection policy and the rules governing the use of digital photos of children as outlined in this policy.

Digital images of children showcasing their academic performance, sports achievements, artistic accomplishments, or similar events must be managed in accordance with the school's child protection policy.

Article 8. Social Media

Social media platforms (e.g., Facebook, Instagram, WhatsApp, LinkedIn, Dropbox, etc.) may be used by school staff in relation to school activities. However, personal social media accounts must not be used for school events or purposes.

The school's public relations manager is responsible for managing the school's official social media accounts and communications conducted through them. Any records posted on the school's official social media channels must be approved in advance by the public relations manager.

When such permission is granted, the school's personal data protection policy must be strictly adhered to.

Article 9. Video Surveillance in the European School Building

Video surveillance is conducted on the premises of the European School, including the outer perimeter of the building, entrances, corridors, canteen cash registers, kitchen, yard, and playgrounds. The purpose of video surveillance is to ensure the safety of school employees, protect school property, safeguard schoolchildren/children, and protect against harmful influences or incidents.

Mandatory video surveillance locations must be marked with appropriate warning signs. In such cases, data subjects must be informed about the processing of their personal data.

Video surveillance is prohibited in cloakrooms, hygiene areas, and specific locations in the kitchen used solely for food preparation and dishwashing purposes. Wired technology used for food-related activities within the school must comply with operational purposes, and employees must be informed of such practices in writing.

The school's IT service is responsible for creating a file system for storing video recordings. This system must include information about the date, location, and time of data processing, in addition to the video recordings themselves. The retention period for data collected through video surveillance is determined by Georgian legislation or, in its absence, by the school's internal regulations.

Video recordings are stored on the server for up to one month (depending on the storage capacity). Access to these recordings is granted to the Security Service and the IT Manager. In the event of a specific incident, the relevant recordings may be extracted and stored on Google Drive, accessible only to the IT Manager.

The school administration or disciplinary committee may access these recordings upon submitting a justified request. Additionally, law enforcement agencies may access the recordings following procedures established by Georgian law. Legal representatives may, if necessary, review recordings on-site while ensuring the protection of others' personal data.

Audio surveillance is permitted only when the school provides remote services or if the subject is informed in advance, with the purpose of improving service quality.

Article 10. Sharing Personal Data

Sharing personal data processed by the school with third parties is prohibited unless there are legal grounds for doing so. Personal data processed by the school may only be transferred to third parties if the transfer is based on grounds provided by Georgian legislation and this policy.

When a request for data transfer is made, the authorized personnel must verify the legality of the request before proceeding.

Article 11. Data Processing for Direct Marketing Purposes

Personal data, regardless of how it is collected or obtained, may only be processed for direct marketing purposes with the explicit consent of the data subject.

Processing data for direct marketing purposes requires the data subject's written consent, including but not limited to their name, surname, address, telephone number, and email address.

Before obtaining consent and engaging in direct marketing, the school must clearly and simply explain to the data subject their right to withdraw consent at any time and the procedure for exercising this right.

Upon receiving a data subject’s request to stop processing their data for direct marketing purposes, the school must cease processing within a reasonable time, and no later than 7 business days. To ensure compliance, the school must maintain a system for managing and tracking the data subject's consent.

The school must provide the data subject with the option to request termination of data processing for direct marketing purposes through the same channel used for direct marketing or another accessible and adequate method.

The method for requesting termination of data processing must be simple and clearly explained to the data subject, including straightforward instructions on how to use it.

The data subject’s right to grant or withdraw consent must be provided free of charge.

The school must document and store records of the data subject's consent and the timing of both the granting and withdrawal of consent. This information must be retained for the duration of direct marketing activities and for one year following the cessation of such activities.

Article 12. Protection of Student Data in Electronic Journals

The electronic journal is a specialized platform (ASAS - quickschools.com; IB - managebac.com; Georgian Program - edupage.org) used for recording student attendance and grades electronically.

In the electronic journal, the following personal data of students is processed: name, surname, assessment, attendance, subject groups, schedule, and school-provided email addresses created by the school's IT manager.

Access to the electronic journal and the personal data it contains is restricted to authorized personnel using individual usernames and passwords. Authorized personnel include the school principal, tutors, subject teachers, level/program coordinators, and the computer center supervisor.

Teachers must avoid transferring student assessments to other files or records to prevent the unauthorized dissemination of personal data. Exceptions are allowed only when it is not feasible to enter marks directly into the journal. In such cases, teachers are required to immediately destroy any records containing student personal data after transferring the information into the electronic journal.

Teachers are obligated to record assessments and attendance directly in the electronic journal without maintaining alternative records.

Access to the data stored in the electronic journal is permitted only when necessary and for a specific purpose. Only individuals with an individual username and password may review the data, ensuring secure access to the platform.

Article 13. Data Protection for Recording Entry and Exit from Premises

To record entry and exit from the school building, the school collects the following data from visitors and employees: name, surname, personal number, date and time of entry and exit, and purpose of visit.

Access to the recorded information about entry and exit is restricted to the following authorized personnel: the director, administrative manager, and security service.

The data specified in this article is retained for one academic semester. After this period, the data must be deleted or destroyed.

Article 14. Data Protection for Email and Phone Numbers

For the purpose of effective communication, the school processes email addresses and phone numbers of employees, pupils, and their parents/legal representatives.

The use of email and phone number data is strictly limited to school activities, such as sharing work-related information with employees and delivering educational content or updates to pupils and parents.

Article 15. Data Protection for Managing Personal Records

To effectively manage the general education process, the school handles personal records of both pupils and employees.

Personal records are securely stored within the school. Responsibility for maintaining and protecting these records is assigned as follows:

- Employees: Managed by the Human Resources (HR) department.
- Pupils: Managed by the Admissions Administration and the Marketing and Communication Manager.

Only authorized personnel have access to the personal records of pupils and employees. These include: the school director, lawyer, and HR (in the case of employees); and the admission administration, marketing and communication service, program coordinator, and the corresponding class tutor (for the personal records of pupils in their tutoring class). Personal data is accessed and used solely for official purposes by authorized personnel, depending on the school's activities. Examples include student admissions, transfers between classes, mobility, or teacher recruitment/dismissal.

To ensure the legal processing of data, periodic monitoring of authorized personnel's activities is conducted.

Personal Data Processed During Pupil Records Management:

- Pupil information: Name, surname, photo, personal number, citizenship, gender, date and place of birth, residential address, phone number, email, academic performance, educational history, health status, and special needs status.
- Parent/legal representative information: Name, surname, personal number, citizenship, gender, date and place of birth, phone number, email, and residential address.
- The personal record of a student is securely stored for 75 years.
- The removal of the original record is allowed only in cases of student mobility as defined by legislation, and only if the receiving school submits a formal written request. It is strictly prohibited to hand over the original record to the student, parent, guardian, or legal representative.
- During the admission-enrollment process, the admission administration, marketing and communication service access the student's health information and relay it to medical personnel for further processing. Health-related information is stored in the medical office and includes medical complaints, dispensation of medicines, and compliance with medical standards for educational institutions. These processes align with the standard operating procedures for medical services in Georgian general education institutions as defined by the

Ministry of Health and Social Affairs (2022). Additionally, personal data is processed in compliance with Joint Order N41/n/01-23/N of March.

- University education advisors have access to students' personal data to provide appropriate foreign curriculum guidance, grant facilitation, and consultation.
- Advisors may also access personal data for authorization and examination purposes, as well as for determining the alignment of foreign education with the national curriculum.

The following personal data of teachers/employees is processed: Name, surname, photo, personal number, citizenship, gender, date and place of birth, residential address, phone number, email, educational background, employment history, criminal record, teacher status, and professional activities.

The financial service and administrative manager have access to the personal data of employees, pupils, and registered applicants. Data usage depends on the specifics of the case.

Article 16. Data Protection in Electronic Database Management

To effectively manage the general education process, the school maintains an electronic database on the portal Eschool.emis.ge.

Access to the electronic database (Eschool.emis.ge) is restricted to authorized individuals, including the school principal, admissions administration, and the marketing and communication service. The data stored in the database is accessed or used exclusively for official purposes by authorized persons, such as during student mobility procedures or when verifying a teacher's workload.

To ensure the lawful processing of data by authorized individuals, periodic monitoring of their activities is conducted.

A school director may address issues related to the protection of a data subject's rights and the processing of their personal data either on their own initiative or based on an application submitted by the data subject.

The following personal data of students is processed within the electronic database:

- Student Information: First name, last name, photo, ID number, nationality, gender, date and place of birth, residential address, telephone number, email, academic performance and educational records, health information, and details about special needs status.
- Legal Representative (Parent) Information: First name, last name, personal number, citizenship, gender, date and place of birth, phone number, email, and residential address.

Additionally, the electronic database processes the following personal data of teachers and employees:

First name, last name, photo, personal number, citizenship, gender, date and place of birth, residential address, telephone number, email, educational background, workplace(s), criminal record information, teacher status, and details of activities undertaken for their professional development.

This structure ensures compliance with legal requirements and promotes the secure and responsible handling of personal data.

Article 17. Personal Data Breach Notification

In accordance with this policy and applicable legislation on personal data protection, the school must implement measures to manage any breach of personal data protection.

All school employees, contractors, and individuals processing personal data for or on behalf of the school are required to report any data breach. This includes providing the date, time, and details of the incident to the school's Personal Data Protection Officer (info@dpo.ge, +995598579350) and the school principal. The report must be made by completing and submitting Annex N3 of this document.

Article 18. European School Commitments

When disclosing data, the data controller and the authorized person must record the following details: which data was disclosed, to whom, when, and on what legal grounds. This information must be stored alongside the data subject's information for the duration of its retention period.

In compliance with Georgian legislation, the school is required to document the following details related to data processing:

A) The identity, name, and contact information of the person responsible for processing, the personal data protection officer, individuals responsible for co-processing, and the authorized persons for processing;
B) The purposes of data processing;

C) The data subjects and categories of data;

D) The categories of data recipients (including recipients in other countries or international organizations);

E) Information on the transfer of data to another country or international organization, including guarantees for data protection and, if applicable, permission from the Personal Data Protection Service;

F) The retention periods for the data, or if a specific period cannot be determined, the criteria for determining its retention period;

G) A general description of the organizational and technical measures implemented to ensure data security;

H) Records of any incidents (if applicable).

The school is obligated to systematically update the information outlined in the first paragraph of this article.

Article 19. Final Provisions

Amendments and additions to this policy may be made based on an order issued by the Director of the European School.

Annex 1

Consent / Confirmation of being informed

On Personal Data Processing and Video Surveillance System

By signing this document, I hereby consent to the processing of my personal data and the personal data of the individual provided by me by “European School” LLC (hereinafter referred to as "the School") in accordance with applicable legislation and the School's regulations. The data includes, but is not limited to: photographs, name, surname, personal identification number, gender, age, phone number, registration address, actual place of residence, email address, special category data, and other personal information.

I also consent to the School requesting, from public and private institutions related to the educational field, the personal data of myself and the individual provided by me, including special health-related data. Such data may be processed as necessary to fulfill the School’s obligations and functions.

The processing of the above-mentioned personal data by the School may involve both contractual and other forms of communication as required for addressing or resolving relevant issues.

Special References:

1. Photo/Video/Audio Material Collection

The School aims to inform a wide audience about its events, including publishing text, photo, video, and audio materials, as well as personal data obtained during school excursions, trips, (sports) competitions, educational projects, open-door days, and other activities, to share information with the general public.

If you agree to the photographing, video recording, or audio recording of the individual specified in this document during the educational process and various school activities, please check the box:

☐

If you do not agree, please mark the following:

☐

2. Publishing Personal Data

If you agree to the publication of the personal data of the individual specified in this document through the following means, please mark the corresponding box:

Information board in the school building

☐

Annual report/School album/Brochures and similar materials

☐

Press (print and electronic versions)

☐

The World Wide Web (Internet), including the School's website (www.europeanschool.ge), Facebook, Instagram, and other school-related social media platforms

☐

Photos

☐

Videos/Audio Material

☐

Other personal data (e.g., last name, first name, etc.)

☐

Granting rights to publish photographs is not subject to reimbursement and includes editing rights, provided that any edits do not result in the data subject being presented in a negative context.

If you or the individual you represent wishes to have photo, video, or audio material removed from the School's website, brochure, or other publications, you may submit a written request to the School at any time.

You have the right, at any time and without explanation, to withdraw this consent for future use. Such withdrawal may apply to specific types of personal data only. However, the withdrawal of consent does not affect cases where the data is processed on other legal grounds. For printed materials, consent cannot be revoked once the printing order has been issued. Upon withdrawal of consent, the relevant data will no longer be used for the specified purposes and will be immediately removed from the internet to the extent possible.

Consent withdrawal requests must be submitted in writing, either in material form or via the School's official email address: info@europeanschool.ge.

Consent is granted voluntarily. No adverse consequences will result from withholding or withdrawing consent.

Additionally, you have the right to access the personal data processed under this consent and to request information about the processed data. You may also request the correction, updating, addition, blocking, deletion, or destruction of such data. Furthermore, you have the right to file a complaint with the State Inspector's Service.

We also inform you that video surveillance is conducted within the school building (including the outer perimeter, entrances, corridors, and working rooms), as well as in the yard and playgrounds. The

purpose of this surveillance is to protect school property, ensure the safety of students, and safeguard against potential harm, as well as for monitoring purposes. The video surveillance system enables direct observation of the relevant areas and records video (including audio) footage. These recordings include information about the date, location, and time of data processing.

The complete document outlining the personal data protection policy is available on the school's website and can also be obtained from the school upon request.

By signing this document, I confirm my consent to the collection, processing, and use of the personal data of the individuals specified herein.

Student: (Full Name)

Personal ID/Passport Number:

Parent/Legal Representative:

(Full Name)

Personal ID/Passport Number:

Signature:

Signature Date: ____ / ____ / 20__

Annex 2

Consent / Confirmation of being informed

On Personal Data Processing and Video Surveillance System

By signing this document, I confirm my consent for “European School” LLC (hereinafter referred to as "the school") to process my personal data in accordance with applicable legislation and school regulations. This consent applies during the recruitment or employment period and includes the following types of data:

- Biographical information
- Identification details
- Educational background
- Contact information
- Criminal record and health-related data (e.g., submitted medical certificates)
- Photograph
- Bank account details
- Employment history
- Information about salary and settlement office
- Performance-related information, including management measurement indicators, evaluations, and comments
- Data regarding entry and exit from the school premises
- Special category data
- Any other personal data provided by me in the documents I have submitted

Furthermore, I consent to the school requesting my personal data, including special category data, from any public or private institution related to the education sector. This data may be processed to fulfill obligations or functions assigned to the school.

The school is authorized to process the aforementioned personal data without limitation for addressing or resolving any issues arising during the course of my contractual or other forms of relationships with the institution.

1. The aforementioned personal data may be transferred to third parties only if legally justified (e.g., for managing employee insurance, wages, pensions, other allowances, payments to mobile service providers, etc.).

2. The personal data of former employees is processed and stored for a period of up to three years.
3. The personal data of potential employees or candidates for employment is processed and stored for no longer than one year.
4. The security and integrity of personal data is a high priority for the school. Appropriate administrative and technical measures are implemented to protect personal data. The school ensures data security by controlling access to buildings, rooms, and cabinets 24/7 where data, computers, media, or printed materials are stored. Personal data is stored within the computer system of authorized personnel, accessible only through appropriate password protection. Servers are safeguarded with voltage regulation systems and wired-interactive uninterruptible power supply (UPS) systems. User access to data is restricted and files are managed with controlled access to folders or drives. The school's ICT department ensures secure access to files stored on fully or partially solid-state drives.

5. The school maintains a database of employee photographs. If you consent to the publication of the personal data specified below, please check the corresponding box: ☐

   ☐ Photo

   ☐ Biographical Data

If you agree to have your photo published on the school website (www.europeanschool.ge) or on other social media platforms, please indicate your consent by marking the appropriate box.

You have the right to withdraw this consent at any time, without providing an explanation. Withdrawal may apply to all or part of the personal data specified. However, the revocation of consent does not affect cases where data processing is carried out on other legal grounds. Consent withdrawal must be submitted via a written application, either in physical form or sent to the school's official email address: info@europeanschool.ge.

Consent is granted voluntarily. Refusal to provide consent or its subsequent withdrawal will not result in any adverse consequences.

Additionally, you have the right to access the personal data processed under this consent. You are also entitled to receive information about the processed data and to request their correction, updating, addition, blocking, deletion, or destruction. Furthermore, you have the right to submit a complaint to the State Inspector's Service.

We would also like to inform you that the school conducts video surveillance within the school building (including the outer perimeter, entrances, corridors, and workrooms), as well as in the yard and playgrounds. The purpose of this surveillance is to ensure the safety of individuals within the school premises, protect school property, and safeguard the security of students/pupils. The video surveillance system allows direct observation of designated areas and records video (including audio) along with information about the date, place, and time of data processing.

The complete personal data protection policy is available on the school's website and can also be obtained upon request from the school.

By signing this document, I consent to the collection, processing, and use of my personal data.

Employed: (Full Name)

Personal/Passport No.:

Signature:

Date of Signature: --------- / -------- / 20__.