DATA PRIVACY NOTICE FOR FEU HIGH SCHOOL STUDENTS

Welcome to the Registrar's Office of FEU High School.

We are dedicated to ensuring that your personal information is handled with the utmost care and in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations, and issuance of the National Privacy Commission, collectively known as the Data Privacy Act.

Our commitment to data privacy is unwavering. We adhere to the highest standards of data protection and privacy, ensuring that all personal data collected is processed lawfully, fairly, and transparently, in accordance with the principles of transparency, legitimate purpose and proportionality. We implement robust security measures to safeguard your information and uphold your privacy rights.

Our role in the privacy of your personal data

We, the Registrar's Office, as the Personal Information Controller (PIC), is responsible for ensuring that the personal data you provide us is processed in accordance with the Data Privacy Act. The Registrar's Office will work closely with the Academic Affairs Office, Academic Services and Student Affairs Office (Student Formation, Student Development, Guidance Office for Counseling, Assessment, Research, and Evaluation, Library, University Health Services, and Bookstore), and Admissions and Financial Assistance for:

1. Scholarship and financial grants
2. Recognition and graduation
3. Academic programs
4. Co-curricular and extra-curricular programs
5. Research purposes
6. Intervention programs
7. Enrollment and annual review or updating of personal records
8. Surveys and occasional school activities in which students' personal information including opinions may be asked

The Registrar's Office will also work closely with the Finance Office, Facilities and Technical Services Office, Information Technology Services Office, Quality Management Office, and Office of the Executive Director for:

1. Finance and accounting purposes
2. Safety and security
3. Office operations

Our key responsibilities include:

1. Data Collection and Processing: Collecting and processing personal data lawfully, fairly, and transparently.
2. Data Security: Implementing robust security measures to protect your personal information from unauthorized access, alteration, or disclosure.
3. Data Accuracy: Ensuring that the personal data we hold is accurate and up to date.
4. Compliance and Accountability: Adhering to all applicable data privacy laws and regulations and being accountable for our data processing activities.

You, as a data subject, you have an important role in maintaining the privacy and security of your personal information. Your responsibilities include:

1. Provide Accurate Information: Ensure that the information you provide to the Registrar's Office is accurate and up to date. This helps us maintain the integrity of our records and deliver better services.
2. Understanding Your Rights: Familiarize yourself with your rights under the Data Privacy Act. These rights include accessing your personal data, requesting corrections, and understanding how your data is being used.

3. Exercising Your Rights: Actively exercise your data privacy rights by contacting us if you have any concerns or requests regarding your personal information. We are committed to addressing your inquiries and ensuring your data is handled appropriately.
4. Protecting Your Information: Take steps to protect your personal information, such as using strong passwords and being cautious about sharing sensitive data.

By fulfilling these responsibilities, we both contribute to upholding the highest standards of data privacy and security.

The personal data we collect and how we use it

We collect various types of personal data at different stages of your interaction with us. The timing of collection, the types of personal data we collect, and the specific purpose and use of your personal data are as follows:

Activity	**Types of Personal Data Collected**	**Specific Purpose**	**Legal Basis**
Enrollment (Registration)	Student name (first name, middle name, last name, nickname), place of birth, citizenship, religion, gender, telephone/cellphone number, language spoken at home, year level, school/campus, present school, address of the school, student permanent address (country, region, house number, street/barangay/village, city/municipality, province, zip code), family details: father (first name, middle name, last name, living or deceased, date of birth, age, citizenship, college/university attended, degree, occupation, position, office name, office address, office telephone number, e-mail address, mobile number), mother (first name, middle name, last name, living or deceased, date of birth, age, citizenship, college/university attended, degree, occupation, position, office name, office address, office telephone number, e-mail address, mobile number), guardian (first name, middle name, last name, relationship to	Student identification and records management, academic administration, financial transaction, student welfare and safety, government compliance and reporting, institutional planning and improvement	Contractual necessity, Legal obligations, legitimate interests

	student, home address, date of birth, citizenship, gender, telephone number, mobile number, e-mail address, occupation, position, office name, office address, office telephone number), track applied for (first choice, second choice), person to notify in case of emergency (name, relationship to student, address, telephone number, mobile number), LRN number		
Enrollment checklist (for new students)	Student's name, date, Adcon number, grade level, strand, voucher type	Tracking of accomplished student enrollment procedure	Contractual necessity
Enrollment checklist (for old students)	Student's name (last name first name, middle name), date, grade level, strand/section, student number	Tracking of accomplished student enrollment procedure	Contractual necessity
Enrollment (Issuance of Certificate of Registration or COR)	Signature over printed name of parent / legal guardian, date signed	Issuance of proof of enrollment	Contractual necessity
Enrollment (Issuance of School I.D.)	Student's photo and signature	student identification and security, access to school services, emergency and safety measures	Contractual necessity, Legal obligations, legitimate interests
Profile updating	Student name (first name, middle name, last name, name extension), active contact number of student, active contact number and e-mail address of parent/legal guardian	Student identification and records management	Contractual necessity
Research	Student's scanned copy of school I.D., signature, e-mail, contact number	Improvement of student services	legitimate interests
Locker application	Student's name, grade level, section	Student verification, service management	Contractual necessity
Disciplinary investigation	CCTV viewing of student	Safety and security, incident investigation	Legal obligations, legitimate interests, vital interests
Library activities	Student's name, grade level, section, and student number	Student verification, service management	Contractual necessity, legitimate interests
Equipment or material requests from Facilities	Student's name and signature	Student verification, service management	Contractual necessity,

and Technical Services Office			legitimate interests
Voluntary student activities and SAILS pre-registration	Student's name, grade level, section	Student verification, service management	Contractual necessity, legitimate interests
Academic advising	Full name and signature of student, full name and signature of parent/legal guardian	Student verification, service management	Contractual necessity, legitimate interests
Special academic request/s	Request letter with parent's/legal guardian's signature, photocopy of parent's/legal guardian's valid ID, medical certificate (if applicable), flight details (if applicable)	Student verification, service management	Contractual necessity, legitimate interests
Change of section request	Request letter with parent's/legal guardian's signature, photocopy of parent's/legal guardian's valid ID	Student verification, service management	Contractual necessity, legitimate interests
Change of Grade 12 specialization request	Request letter with parent's/legal guardian's signature, photocopy of parent/legal guardian's valid ID	Student verification, service management	Contractual necessity, legitimate interests
Evaluation forms of school offices	Student's name, grade level, section, student number, FEU HS e-mail address, contact number, signature	Improvement of student services	legitimate interests
Enrollment cancellation, withdrawal, dropping, and transfer-out	Date applied, student's personal information (last name, given name, middle name), student's contact information (telephone number, mobile number, e-mail address), academic information (I.D. number, strand, level and section), parent's/legal guardian's information (full name, e-mail address, contact number, relationship to student), school information (name of school transferring to, address), reason for enrollment cancellation, withdrawal, dropping, and transfer-out, student's signature over printed name, parent's/legal guardian's signature over printed name	Student identification and records management, government compliance and reporting	Contractual necessity, legal obligations, legitimate interests

Refund	Letter for refund, photocopy of student's I.D., photocopy of parent's or legal guardian's valid I.D., bank details (account name, account number, bank certificate)	Student verification and financial records	Contractual necessity
Academic gown/toga form	Student's name (last name, given name, middle initial), student number, grade level, strand and section, height	Student verification	Contractual necessity
Document request form and college application form	Student's name (first name, middle initial, last name), student number, grade level, contact number, e-mail address, document type, list of requested documents, purpose, name of school)	Student identification and records management, improvement of student services	Contractual necessity, legitimate interests
Claiming of document requested from the Registrar's Office	Date, student's name, document requested, signature	Student identification and records management	Contractual necessity
Early dismissal form	Full name and signature of student	Student verification, safety and security	Contractual necessity, vital interests

These purposes and legal bases ensure that your personal data is processed lawfully, fairly, and transparently, in accordance with the principles of transparency, legitimate purpose, and proportionality as mandated by the Data Privacy Act.

Recipients of your personal data

We engage third-party service providers to process personal data on our behalf. These third parties are carefully selected and are required to comply with the Data Privacy Act and our data protection policies.

Transmission of personal data to service providers for services such as enrollment transactions, access to library resources, class activities, other campus life activities, security, medical exams, insurance provider, exams/assessments, work-immersion, curricular, co-curricular activities, extra-curricular activities, and commencement activities are appropriately covered by an outsourcing agreement with provisions for data privacy as required by the Data Privacy Act of 2012.

Personal data storage, retention and disposal

We are committed to ensuring secure storage, appropriate retention, and proper disposal of your personal data.

Your personal data is stored in a secure location.

Personal data is stored secure locations, which may include:
a. On-Premises Servers: Data is stored on secure servers located within our facilities. These servers are protected by physical security measures, such as access control systems, surveillance cameras, and security personnel.
b. Cloud Storage: We use reputable cloud service providers to store personal data. These providers are selected based on their compliance with data protection standards and their ability to implement robust security measures.
c. Backup Storage: Regular backups of personal data are performed and stored in secure offsite locations to ensure data availability and integrity in case of physical or technical incidents.

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required by law.

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, or as required by law. Our retention policies are guided by the following principles:

a. Purpose Limitation: Personal data is retained only for the duration necessary to achieve the specific purposes for which it was collected.
b. Legal Compliance: We comply with legal and regulatory requirements regarding the retention of personal data, including mandatory retention periods.
c. Data Minimization: We regularly review the personal data we hold and ensure that it is accurate, relevant, and limited to what is necessary for the purposes for which it is processed.

When personal data is no longer required, we ensure its secure and irreversible disposal. Our disposal practices include:

a. Data Deletion: Personal data stored electronically is securely deleted using methods that prevent recovery, such as data wiping and degaussing.
b. Physical Destruction: Personal data in physical form, such as paper records, is shredded or incinerated to prevent unauthorized access.
c. Third-Party Disposal: When using third-party service providers for data disposal, we ensure they comply with our data protection standards and legal requirements.

Security of personal data

We recognize that the processing of personal data involves various risks that could potentially impact on the privacy and security of individuals. We have identified key risks and implemented robust security measures to mitigate these risks.

1. Possible Risks in the Processing of Personal Data
a. Data Breaches: Unauthorized access, disclosure, alteration, or destruction of personal data due to cyber-attacks, hacking, or other malicious activities.
b. Accidental Data Loss: Loss of personal data due to human error, system failures, or natural disasters.
c. Unauthorized Access: Access to personal data by unauthorized personnel, including employees or third-party vendors.
d. Data Misuse: Improper use of personal data for purposes other than those for which it was collected, leading to privacy violations.
e. Regulatory Non-Compliance: Failure to comply with data protection regulations, resulting in legal penalties, fines, and reputational damage.

To mitigate these risks, we have implemented a range of organizational, physical and technical security measures:

2. Security Measures to Address Risks
To mitigate these risks, we have implemented a range of organizational, physical and technical security measures:

a. Organizational Security Measures
* Information Security Policies: We have established comprehensive information security policies that outline our commitment to protecting personal data. These policies are regularly reviewed and updated to reflect the latest security practices and regulatory requirements.
* Employee Training: All employees undergo regular training on data protection and information security best practices, ensuring they are aware of their responsibilities and the importance of protecting personal data.
* Incident Response Plan: We have a robust incident response plan in place to address any security breaches or incidents promptly, including procedures for identifying, containing, and mitigating the impact of security incidents.
* Third-Party Security: We ensure that any third-party service providers who process personal data on our behalf comply with our security standards and legal requirements, including conducting due diligence and regular audits of their security practices.

b. Physical Security Measures
* Secure Facilities: Personal data is stored in secure facilities with physical security controls, such as access control systems, surveillance cameras, and security personnel.
* Data Backup and Recovery: We implement regular data backup procedures to ensure that personal data can be restored in the event of a physical or technical incident, including off-site storage of backup data to protect against data loss.

c. Technical Security Measures
* Data Encryption: We use advanced encryption technologies to protect personal data both in transit and at rest, ensuring its confidentiality and integrity.
* Access Controls: Access to personal data is restricted to authorized personnel only, using role-based access controls and regular reviews of access rights.
* Firewalls and intrusion Detection Systems: We employ firewalls and intrusion detection systems to monitor and protect our networks from unauthorized access and potential threats.
* Secure Software Development: Our software development practices include security-by-design principles, ensuring that security is integrated into our systems and applications from the ground up.
* Regular Security Audits: We conduct regular security audits and vulnerability assessments to identify and address potential security risks.

We are committed to continuously improving our security measures to keep pace with evolving threats and technological advancements. This includes:
a. Regular Testing: Conducting regular testing of our security measures, including penetration testing and security assessments, to ensure their effectiveness.
b. Compliance Monitoring: Monitoring compliance with our security policies and procedures through regular audits and reviews, and promptly addressing any identified areas for improvement.

Your rights as a data subject

Under the Data Privacy Act, you are entitled to specific rights as a data subject. These rights empower you to have reasonable control over your personal data. Your rights and how you can exercise them are enumerated and described as follows:

1. Right to Be Informed
You have the right to be informed about the collection and processing of your personal data. This includes information about the purpose of data processing, the scope and method of processing, the recipients of the data, and the period for which the data will be stored.

How to Exercise:
a. Request information from the data controller about how your personal data is being processed.
b. Review the privacy notice provided by the organization collecting your data.

2. Right to Access
You have the right to access your personal data. This includes the right to obtain a copy of the data and information about how it is being processed.

How to Exercise:
a. Submit a written request to the data controller to access your personal data.
b. Specify the information you wish to access and provide any necessary identification documents.

3. Right to Rectification
You have the right to request the correction of inaccurate or incomplete personal data.

How to Exercise:
a. Contact the data controller and provide the correct information.
b. Submit a written request for rectification, including any supporting documents.

4. Right to Erasure or Blocking
You have the right to request the deletion or blocking of your personal data under certain conditions, such as when the data is no longer necessary for the purposes for which it was collected or when you withdraw consent.

How to Exercise:
a. Submit a written request to the data controller specifying the reasons for the request.
b. Provide any necessary identification documents and supporting evidence.

5. Right to Object
You have the right to object to the processing of your personal data, particularly if the processing is based on legitimate interests or for direct marketing purposes.

How to Exercise:
a. Submit a written objection to the data controller, specifying the grounds for the objection.
b. Provide any necessary identification documents.

6. Right to Data Portability
You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit it to another data controller.

How to Exercise:
a. Submit a written request to the data controller for data portability.
b. Specify the format in which you wish to receive your data and the recipient data controller.

7. Right to Damages
You have the right to claim compensation for any damage suffered due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal data.

How to Exercise:
a. File a complaint with the National Privacy Commission (NPC) or the appropriate court.
b. Provide evidence of the damage suffered and any supporting documents.

8. Right to File a Complaint
You have the right to file a complaint with the National Privacy Commission if you believe that your data privacy rights have been violated.

How to Exercise:
a. Submit a written complaint to the NPC, detailing the nature of the violation.
b. Provide any necessary identification documents and supporting evidence.

Transmissibility of your Rights

Your rights as a data subject can be transmitted to your legal assignees or lawful heirs. This ensures that personal data remains protected even after your death.

How to Exercise:
a. Legal assignees or heirs must provide legal evidence to support their claim.
b. Submit a written request to the data controller or the NPC, as applicable.

For your inquiries regarding the processing of personal information stated in this Privacy Notice, as well as, any concerns or complaints regarding data privacy, or the exercise of your rights as a data subject under Data Privacy Act, you may contact the Data Protection Officer at:

The Data Protection Officer
FEU High School, Inc.
Nicanor Reyes Street, Sampaloc, Manila
Landline: 8849-4000 loc. 801
Email: dpo@feuhighschool.edu.ph