PRIVACY POLICY

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY BANGALORE

UPDATED IN DECEMBER 2024

Contents

PRIVACY POLICY

INTRODUCTION

This Privacy Policy outlines the practices of IIIT-B in collecting, processing, storing, and sharing personal data of our faculty, staff, students, and other associated individuals. IIIT-B is committed to upholding the privacy rights of all stakeholders in compliance with global privacy standards and the privacy regulations of the Government of India. This policy aims to protect the confidentiality, integrity, and accessibility of personal data managed by the institution.

DEFINITIONS OF PERSONAL DATA

1. Faculty

Personal data of faculty members includes information such as name, contact details, qualifications, employment history, research publications, personal mobile numbers, performance records, any biometric data where applicable and health data including blood group. This data is collected for academic, administrative, life-saving emergencies and regulatory purposes.

2. Staff

Staff personal data includes name, contact details, employment details, professional qualifications, performance records, any biometric data where applicable, health data including blood group and other work-related information essential for managing administrative functions, life-saving emergencies and regulatory purposes

3. Students

For students, personal data encompasses name, identification number, academic records, contact details, and health information as needed for academic, administrative, life-saving emergencies and regulatory purposes. Data specific to the requirements of differently-abled students is also managed with a focus on accessibility and inclusion.

To the extent that we are able to ascertain age, we only process information about minors under the age of 18, with the consent of the parents or legal guardians or when the information is provided to use by the parents or legal guardian.

4. Differently-Abled Students

Additional personal data is collected to facilitate accessibility and accommodations. This includes health records, mobility requirements, and academic adjustments required for inclusive education.

5. Parents

Parent or guardian data, such as contact details and relationship to the student, is maintained for emergency purposes and communication concerning the student's welfare.

6. Visitors

When individuals visit the Institute in-person information such as name, mobile number, email address, residential/ office address and purpose of the visit may be collected. These information shall also be processed and governed as per this policy.

7. Other Data

Gender-based Data

Sensitive personal data related to any gender-specific requirements are handled with confidentiality and shared only when essential for institutional support or safety. Such data is only collected and handled by the concerned authorities or the Gender Cell of the institute.

Religion and Caste based Data

The institute follows a strict non-discrimination policy regarding religion, caste, or creed and, therefore, does not routinely collect data related to these attributes. However, the institute may collect this information from students or other personnel when required to facilitate government programs, such as scholarships provided by the Government of India or State Governments. This data is kept strictly confidential and is used exclusively for the intended purpose.

DATA SHARING PROTOCOLS

Personal data is shared only when required by institutional needs and on a strict need-to-know basis. Internally, data may be accessed across departments solely to fulfill specific institutional requirements. Externally, personal data is shared only with explicit consent from the individual, or when mandated by legal or regulatory obligations. All personnel are responsible for safeguarding the confidentiality of personal data and must adhere to the institute's data protection policies and practices.

DEPARTMENT-SPECIFIC PRIVACY POLICIES

1. Finance
Personal data in the Finance Department includes banking information, payroll records, and fee transactions. This data is strictly controlled and shared only with authorized personnel.

2. Administration
The Administration Department holds data on employment, contact details, and other operational information. Only necessary information is accessible to administrative staff as required.

3. Academics
Academic departments handle data on students' academic records, grading, and course enrollments. Academic information is shared with faculty and respective students only for relevant academic purposes. Such data is shared with external agencies only for the purpose of employment / recruitment or such other administrative requirements.

4. Sports
Sports-related personal data includes fitness levels, health conditions relevant to participation, and performance metrics. This data is accessible only to sports coordinators and relevant medical staff.

5. Extracurricular Activities
Information on extracurricular participation, achievements, and personal preferences is recorded for activity planning and is restricted to activity coordinators and advisors.

6. Health
Health data, including blood group and specific medical requirements, is maintained confidentially and accessed only by authorized medical or counseling staff, particularly for emergency care.

DATA SHARING IN SPECIAL CASES

In cases where data sharing is necessary for legal, medical, or safety purposes, IIIT-B will take all reasonable measures to protect privacy. Only minimum information required will be shared, with a clear purpose and record of sharing maintained. For official requests from external authorities, data will be shared as per legal requirements.

SHARING OF MOBILE NUMBERS AND EMAIL IDS

Sharing mobile numbers and email IDs in the institute should be carefully controlled, given their potential to impact privacy if shared too broadly

1. Purpose-Based Access

- **Internal Use Only:** Mobile numbers and email IDs should be used primarily for internal communication within the institute and shared only when necessary to fulfill specific roles and responsibilities.
- **Student-Related Communications:** Faculty and administrative staff may have access to student contact details for academic advising, administrative notices, and emergency purposes.

2. Consent-Based Sharing

- **Explicit Consent:** Personal contact information should only be shared externally (outside the institution) with the explicit consent of the individual, unless legally required.
- **Directory or Publication Restrictions:** Mobile numbers and email IDs should not be published on public platforms or directories accessible to individuals outside the institution unless consent is obtained.

3. Limited Access by Departments

- **Academic and Administrative Staff:** Only faculty, academic mentors, and necessary administrative personnel should have access to student contact information.
- **Finance Department:** Should only access contact information when required for financial inquiries or clarifications.
- **Health Services and Emergency Situations:** Medical or counseling staff who are often outsourced staff may be given access to contact details only for health-related follow-ups or emergencies, with the explicit permission of concerned authorities.

4. Security Measures and Confidentiality

- **Data Protection:** Mobile numbers and email addresses should be stored securely, accessible only to authorized personnel, and protected from unauthorized access.
- **Confidentiality Agreements:** Staff members should be briefed on maintaining confidentiality and using contact information solely for official purposes.

5. Sharing for Official External Requests

- **Legal Compliance:** Contact information may be shared with external authorities only when legally mandated (e.g., law enforcement, court orders).
- **Notification of Individuals:** Whenever feasible, notify the individual about the information shared, unless prohibited by law.

DATA RETENTION AND DISPOSAL POLICY

The data retention and disposal policies are appended below:-

1. Employee Records

- **Basic Employment Records** (e.g., job applications, resumes, contracts, payroll records, performance appraisals):
  - **Retention Period**: Typically 7 years after termination of employment.
  - **Purpose**: Compliance with employment and tax laws, reference for future employment verification, and resolving any legal claims.

- **Disciplinary Records**:
  - **Retention Period**: Often kept for 3–5 years after the issue is resolved, or for 7 years after employment ends.
  - **Purpose**: To maintain records for potential legal defense or employment history reviews.

- **Financial and Payroll Information**:
  - **Retention Period**: Generally, 7 years to meet tax and financial record-keeping requirements.
  - **Purpose**: For audit purposes, compliance with tax laws, and supporting wage or benefit claims.

- **Retirement Records**:
  - **Retention Period**: Indefinitely or for as long as needed to verify employee benefits etc.
  - **Purpose**: Necessary to verify retirement benefits claims and for audit purposes.

2. Student Records

- **Academic Records** (e.g., transcripts, enrollment records, degrees awarded, and answer booklets):
  - **Retention Period**: Indefinite, as students may request transcripts years after graduation. However answer booklets of various exams may be destroyed (in accordance with UGC norms) by a duly formed committee by the Director after a duration of six months from the completion of an examination.
  - **Purpose**: For future reference, verification of academic credentials, and institutional records.

- **Financial Aid / Scholarship Records**:

- **Retention Period**: Generally, 3–5 years after the end of the graduation year.
- **Purpose**: Compliance with financial aid regulations and audit requirements.

- **Student Financial Records** (e.g., tuition payments, refunds):
  - **Retention Period**: Typically, 7 years.
  - **Purpose**: For audit, compliance with financial regulations, and resolution of any financial disputes.

- **Disciplinary Records**:
  - **Retention Period**: Often 3–7 years after graduation or resolution of the issue.
  - **Purpose**: For internal record-keeping, handling any post-graduation inquiries, or compliance with legal requests.

3. General Administrative Records

- **General Correspondence and Communication Records**:
  - **Retention Period**: 2–5 years, depending on relevance.
  - **Purpose**: For administrative reference, institutional memory, or legal documentation if necessary.

- **Legal and Compliance Documentation** (e.g., policies, contracts):
  - **Retention Period**: At least 7 years, with some records (like major contracts or compliance audits) kept indefinitely.
  - **Purpose**: To maintain a legal history and ensure compliance with institutional and legal obligations.

ACCESS AND ABILITY TO CORRECT YOUR PERSONAL DATA

The students, faculty, or staff wish to confirm, access or correct the personal information are required to send a written communication request to the Institute DPO, and upon producing an acceptable Government issued proof of identity, the same will be processed within a period of 30 days as per the Privacy Policy of the Institute.

INFORMATION STORAGE AND PROCESSING

The Institute is committed to keeping all information collected from students, faculty and staff secure. In order to prevent unauthorised access to or disclosure of your data, physical, electronic and managerial procedures are put in place to safeguard and secure the information collected online. The personal information

will be stored and processed only for the purpose for which it is collected as mentioned. The Institute may store information in the data servers located physically inside the Institute or in a secure cloud storage availed by the Institute for the purpose of processing.

PRIVACY POLICY OF INSTITUTE WEB SITE

When visitors browse Institute web site, personal information such as name, mobile number, email address, residential/ office address and purpose of the visit may be collected. In case of visit of the Institute web site, cookies may be planted with explicit consent from the users, storing information such as the Internet Protocol (IP) address of the device, date and time of visit. These information shall also be processed as per this policy.

Our Institute website may contain links to other websites of interest. However, once the user accesses these links to leave the Institute web site, users should note that the Institute does not have any control over that other website. Therefore, the Institute is not responsible for the protection and privacy of any information which the user may provide whilst visiting such sites. The users should exercise caution and look at the privacy statement applicable to the linked sites accordingly.

DESTRUCTION/DISPOSAL OF PHYSICAL RECORDS/DATA

Destruction/Disposal of physical records/Data should be done by shredding after following above norms. The disposal is to be done by a duly constituted committee by the Director. The disposed shredded material may be auctioned or sold to private vendors for further disposal.

PROCEDURE FOR GRIEVANCE REDRESSAL

Any grievance with regard to personal information should be addressed to the Data Protection Officer at: dpo@iiitb.ac.in . The grievance raised will be resolved within a period of 30 days from the date of receipt. For grievances which has not been addressed by DPO in a reasonable amount of time, kindly email to iiitbombudsman@iiitb.ac.in

CONTACT INFORMATION OF DATA PROTECTION OFFICER

Data Protection Officer
International Institute of Information Technology Bangalore
26/C Electronic City, Hosur Road
Bengaluru 560 100

Email: dpo@iiitb.ac.in
Phone: 080-4140 7777

This document is approved by the concerned authorities of the International Institute of Information Technology Bangalore