



UNIVERSITY OF YORK MUMBAI

Privacy Policy

Introduction

This Privacy Policy ("**Policy**") outlines how University of York, Mumbai, an independent legal entity operating as a Joint Venture in India (hereinafter referred to as 'the University' or 'India Campus'), collects, processes, stores, and protects Personal Data of individuals ("**Data Principals**") in accordance with the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") and its rules. India Campus acts as an independent Data Fiduciary for data processing activities conducted within its jurisdiction and the data may be exchanged between the India Campus and University of York, UK.

Capitalized terms in this Policy shall have meaning as defined under the DPDP Act.

1. Objectives and Legal Basis

- 1.1. This Privacy Policy sets out the principles, governance framework, and institutional practices adopted by University of York, Mumbai ("**University**") for the processing of Personal Data.
- 1.2. This Policy applies to Personal Data processed in the course of the University's academic, administrative, research, and related functions in India. It embodies the University's approach to privacy and data protection as an important component of institutional governance and accountability.
- 1.3. This Policy is implemented pursuant to laws governing privacy and the protection of Personal Data in India, including specifically, the Digital Personal Data Protection Act, 2023, and shall be interpreted in accordance with applicable Indian law.
- 1.4. This Policy governs and is binding on all academic, administrative, operational, and support functions of the University in India.

2. Scope and Application

- 2.1. This Policy applies to the processing of Personal Data relating to:
- (a) program applicants;
 - (b) enrolled students and alumni;
 - (c) faculty, staff, consultants, and visiting academics;
 - (d) researchers, collaborators, and academic partners;
 - (e) visitors and other individuals engaging with the University who engage with the University through its physical premises, websites, online portals, learning management systems, mobile applications, email communications, social media platforms, events, helplines, CCTV systems, or any other official digital or physical interface operated by the University.
- 2.2. This Policy applies to Personal Data processed through physical records, electronic systems, institutional platforms, and third-party systems used for University functions.
- 2.3. "This Policy does not apply to anonymised data where individuals are not identifiable."

3. Role of the University

- 3.1. The University may collect Personal Data directly from Data Principals as well as receiving Personal Data from third parties under circumstances permitted by law (where Data Principals have given their consent, or otherwise as permitted under the DPDP Act).
- 3.2. The University may also process Personal Data through third-party data processors acting on behalf of the University, who are engaged subject to contractual and organisational safeguards consistent with applicable law.

4. Privacy Governance and Accountability

- 4.1. The University shall maintain an internal privacy governance framework to ensure lawful and responsible processing of Personal Data, including:
- (a) designation of a Grievance Officer for India (see section 14 of this Policy);
 - (b) assignment of responsibilities for privacy compliance within the University's administrative structure;
 - (c) coordination between academic, administrative, IT, and legal functions;
 - (d) documented procedures for grievance redress, handling data principal requests, and managing incident response.

- 4.2. The University shall ensure appropriate awareness and responsible handling of data through guidance and training for staff and administrators involved in processing Personal Data.
- 4.3. Operational procedures, standards, and guidelines supporting this Policy (e.g. grievance redressal, handling of data principal requests, and Personal Data Breach management) shall be implemented by the University by assigning responsibilities to designated administrative, IT, and legal functions.

5. Categories of Personal Data and Data Minimisation

- 5.1. Depending on the context of engagement with an Data Principal, the University may process Personal Data including:
 - (a) identification and contact information;
 - (b) academic records, assessments, and student administration data;
 - (c) employment, professional, and human-resources-related information;
 - (d) financial and transactional data;
 - (e) health, accessibility, or welfare-related information where required;
 - (f) images, recordings, and security-related data (including CCTV);
 - (g) IT system credentials, logs, and access-related information.
- 5.2. The University recognizes that certain categories of Personal Data processed by the University, including health-related information, financial information, and security-related data, may require enhanced safeguards due to their nature and potential impact on Data Principals, and adopts measures to handle such data accordingly.
- 5.3. **Data minimisation:** Personal Data collected and processed shall be limited to what is necessary for legitimate institutional purposes and shall not be retained or used beyond such purposes.
- 5.4. **Student records:** Student academic and administrative records shall be categorised and processed with particular care, recognising their sensitivity, long-term relevance, and potential impact on Data Principals.

6. Purposes of Processing

Personal Data may be processed for purposes including:

- (a) admissions, enrolment, teaching, assessment, and academic administration;
- (b) student support, welfare, discipline, and campus safety;

- (c) employment, faculty administration, and professional engagement;
- (d) research activities and academic collaborations;
- (e) statutory, regulatory, accreditation, and reporting obligations;
- (f) operation, maintenance, and security of IT systems and facilities;
- (g) alumni engagement and institutional communications;
- (h) compliance with lawful requests from public authorities or courts.
- (i) "direct marketing, newsletters, and promotional communications, subject to consent where required."

7. Legal Basis for Processing

- 7.1. Personal Data is processed in accordance with the DPDP Act on one or more of the following bases as contemplated under Section 7:
 - (a) consent, where required under law;
 - (b) legitimate uses permitted under applicable law, including for purposes of employment;
 - (c) compliance with legal or regulatory obligations including those relating to academic, administrative, or other functions of the University.
- 7.2. Where processing is based on consent, it shall be informed, specific, unambiguous, and freely given consent, given clearly and voluntarily, specific to the purpose of which the data principal has been notified and without hidden, ambiguous or forced conditions. Data Principals may withdraw consent in accordance with applicable law, without affecting the legality of processing based on consent before it has been withdrawn. Data Principals must be notified that withdrawal of consent may affect the University's ability to provide certain services or fulfil academic or administrative obligations where such processing is necessary. The University may facilitate the management of consent through a 'Consent Manager' registered with the Data Protection Board of India, where applicable.

8. Children's Personal Data

Where the University processes Personal Data relating to Data Principals below the age prescribed by law, such processing shall be undertaken in compliance with applicable consent, verification, and protection requirements under the DPDP Act and related rules. Where required, the University shall implement reasonable efforts to verify parental or lawful guardian consent prior to processing Personal Data of children.

9. Disclosure and Sharing of Personal Data

9.1. Personal Data may be disclosed, where necessary and lawful, and in compliance with the DPDP Act, to:

- (a) service providers and vendors supporting University functions, under contractual arrangements including Data Processing Agreements (DPAs);
- (b) University of York, UK to comply with its internal processes, procedures, and policies associated the delivery of academic programs and related activities;
- (c) academic institutions, research partners, and collaborators;
- (d) regulators, government authorities, or courts, where required by law;
- (e) professional advisors, auditors, and consultants.

Vendors are subject to due diligence, contractual confidentiality obligations, and security requirements proportionate to the nature of the Personal Data shared.

9.2. Disclosures are limited to what is necessary, aligns with the purpose communicated to the Data Principals, and are subject to appropriate safeguards.

9.3. Within the University, Personal Data is shared with University Personnel only on a need-to-know basis, and subject to access controls and other IT security safeguards.

10. Cross-Border Transfers

10.1. Personal Data may be transferred outside India, given the international nature of higher education and academic collaboration, the University's affiliation with University of York, UK as well as with global third-party service providers (including cloud providers) engaged by the University.

10.2. Any such international transfers shall be carried out in accordance with applicable Indian law (including the DPDP Act and its rules), and subject to contractual, technical, and organisational safeguards adopted by the University, and the recipient entities via appropriate Data Processing Agreements (DPAs) to ensure continued protection of Personal Data in line with the DPDP Act standards.

11. Information Accuracy, Classification, and Security

- 11.1. The University shall take reasonable steps to ensure that Personal Data processed is accurate, complete, and up to date, having regard to the purpose of processing.
- 11.2. Technical and organisational measures are implemented to protect Personal Data, in compliance with the DPDP Act and its rules, and the obligation to maintain reasonable security safeguards and practices, including preventing Personal Data Breaches. These measures are regularly reviewed and updated to address evolving risks.
- 11.3. The University maintains information classification and security frameworks under its IT Security and Information Management Policies. Information classification standards, access controls, and security measures supporting this clause are defined and implemented through the University's IT Security Policy and related standard operating procedures.

12. Data Retention, Lifecycle Management, and Disposal

- 12.1. Personal Data shall be retained only for as long as necessary to serve the specific purpose for which such data was collected from the Data Principal, which is usually for academic, administrative, legal, or regulatory purposes.
- 12.2. If a Data Principal submits a request for erasure of their Personal Data, the University shall promptly comply with this request, unless retention is necessary for compliance with any law for the time being in force or for the exercise of legal claims.
- 12.3. Retention periods vary by data category and function, and are governed by internal retention schedules and disposal procedures, subject to applicable law including the DPDP Act.
- 12.4. Lifecycle management: The University manages Personal Data across its lifecycle, from collection and active use through secure disposal or erasure, and shall ensure that Personal Data is deleted or anonymised when no longer required for the purpose for which it was collected or lawfully permitted to be retained.
- 12.5. Where litigation, regulatory inquiry, or audit is anticipated or ongoing, the University may retain relevant Personal Data beyond standard retention periods.

13. Rights of Individuals (Data Principals) (Data Principals)

- 13.1. Subject to applicable law, Data Principals may have the following rights relating to their Personal Data:

- (a) access Personal Data;
 - (b) request correction of inaccurate or incomplete Personal Data;
 - (c) request erasure of Personal Data where legally permissible;
 - (d) raise concerns or complaints regarding Personal Data processing.
- 13.2. Data Principals may nominate another person to exercise their rights under applicable law in the event of death or incapacity.

14. Grievance Redressal

- 14.1. The University has appointed a Grievance Officer to address concerns relating to Personal Data processing. The Registrar shall serve in this capacity and shall be responsible for receiving, reviewing, and resolving grievances in accordance with applicable data protection laws and institutional policy.
- 14.2. Data Principals may address their concerns relating to privacy or data protection or the subject matter of this Policy to the Grievance Officer:
- (a) Via the website portal
 - (b) Via email; or
 - (c) Via a physical application submitted at the office of the Grievance Officer
- 14.3. The Grievance Officer shall respond to inquiries within the timelines stipulated under the DPDP Act. If a Data Principal is not satisfied with the response or resolution provided by the Grievance Officer, they have the right to approach the appropriate authority under applicable law.

15. Personal Data Breach Management

- 15.1. The University shall maintain documented procedures to identify, assess, and respond to actual or suspected Personal Data Breaches, and shall investigate such incidents and take appropriate remedial and notification actions in accordance with applicable law.
- 15.2. Personal Data Breach response is governed by the University's IT Security Incident Response Standard Operating Procedure. Technical investigation and containment of incidents are coordinated by the University's IT function, while assessment of legal obligations and any required notifications to authorities or affected Data Principals are coordinated by the University's legal or compliance function.

- 15.3. In the event of a Personal Data Breach likely to cause harm, the University shall notify the Data Protection Board of India and affected Data Principals in accordance with statutory timelines.

16. Policy Review and Updates

- 16.1. This Policy shall be reviewed and updated periodically to reflect changes in law, institutional practices, or to accommodate risk assessments.
- 16.2. The current version of this Policy shall be made available to all stakeholders through official University channels.

17. Non-Compliance of this Policy

- 17.1. Any failure to comply with this policy will be taken seriously. Employees found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment, depending on the severity and recurrence of the non-compliance.
- 17.2. Employees are encouraged to report any instances of non-compliance with this policy to the appropriate channels, such as the Data Protection Officer (DPO). Reports will be investigated promptly, and appropriate actions will be taken.