BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI
DATA PRIVACY POLICY

1. INTRODUCTION

The Birla Institute of Technology and Science, Pilani (BITS Pilani), a deemed to be university under Section 3 of the UGC Act, 1956, and recognized as an Institute of Eminence (IoE) by the Ministry of Education, Government of India, is committed to safeguarding the Personal Data entrusted to it by individuals who engage with the Institute in various academic, administrative, operational, and collaborative capacities. This includes applicants, students, faculty, staff, alumni, research collaborators, employees, contractors, suppliers, clients, partners, and other individuals who interact with BITS Pilani across its campuses in Pilani, Goa, Hyderabad, Mumbai and Dubai, as well as through its digital platforms such as BITS Digital and the Work Integrated Learning Programmes (WILP) division.

As a premier higher education institution, BITS Pilani recognizes the importance of protecting Personal Data in accordance with applicable laws and regulations, including the Digital Personal Data Protection Act, 2023 (DPDPA) and Digital Personal Data Protection Rules 2025 ("DPDP Rules") of India. This Data Privacy Policy outlines the principles and practices adopted by the Institute to ensure responsible data processing, uphold the privacy rights of individuals, and maintain high standards of data protection across all academic, research, administrative, and institutional functions.

2. SCOPE

This Policy applies to all individuals and entities who process Personal Data on behalf of the Birla Institute of Technology and Science, Pilani (BITS Pilani), including but not limited to employees, faculty, staff, contractors, vendors, research collaborators, and third-party service providers (“you”, “your”). It governs the processing of Personal Data across all BITS Pilani campuses - Pilani, Goa, Hyderabad, Mumbai and Dubai - as well as its digital platforms such as BITS Digital and the Work Integrated Learning Programmes (WILP) division.

This Policy covers all forms of Personal Data, regardless of the medium in which it is stored (physical or digital) or the method by which it is processed (automated or manual). It is designed to ensure consistent data protection standards across the Institute.

Individual BITS Pilani campuses or divisions may adopt their own Data Privacy Policies, provided that such policies are no less stringent than this Institute-wide Policy and do not conflict with or derogate from the requirements set forth herein.

In addition to the Applicable Laws of India, where the Institute processes Personal Data through a campus, operation, or digital platform situated outside India including its Dubai campus, such processing shall also be subject to the data protection and privacy laws of that jurisdiction, including Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data of the United Arab Emirates ("UAE PDPL") and, where applicable, free-zone specific regimes such as the Dubai International Financial Centre Data Protection Law No. 5 of 2020.

3. DEFINITIONS

A. "Birla Institute of Technology and Science, Pilani" or "BITS Pilani" is a society incorporated under the Rajasthan Societies Registration Act, 1958, and is a deemed to be a University established vide Sec.3 of the UGC Act, 1956 under notification # F.12-23/63.U-2 of June 18, 1964, and have been granted the status of Institute of Eminence by Ministry of Education having its registered office at Vidya Vihar, Pilani (Jhunjhunu) Rajasthan, India, PIN-333031. For the purpose of this Policy the term "BITS Pilani" is deemed to include any and all Institutes.

B. "BITS Pilani Campuses" or "Institute" or refers to all academic and administrative units of the Birla Institute of Technology and Science, Pilani, including its campuses at Pilani, Goa, Hyderabad, andMumbai, and its off-shore campus situated in Dubai, United Arab Emirates. The term also refers to the Work Integrated Learning Programmes (WILP) Division and BITS Digital—the Institute's digital education platform offering online degree and certificate programmes. This definition collectively encompasses all physical and digital entities operated by BITS Pilani for academic, research, and administrative purposes.

C. "**Applicable Laws**" means any applicable federal, state and sectoral laws, regulations and supervisory authority guidelines related to the processing of the Personal Data, cybersecurity practices, and data breach reporting, including but not limited to the Digital Personal Data Protection Act, 2023 of India ("**DPDPA**") and Digital Personal Data Protection Rules 2025 ("DPDP Rules") of India and the European Union General Data Protection Regulation ("**GDPR**") and in respect of the Institute's Dubai campus, the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data ("**UAE PDPL**") and any applicable free-zone data protection regime.

D. "Personal Data" means any information relating to an identified or identifiable natural person.

E. "**Sensitive Personal Data**" shall have the meaning set forth under Applicable Law and where no such categorization of Personal Data is made under the Applicable Law, shall mean any Personal Data, the processing of which is likely to have an impact on the rights and freedoms of the Data Principals (For example, national ID numbers, biometric

information, financial instrument details, medical records, and other data that may require enhanced protection due to its nature or context.)

F. **"Processing"** means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

G. **"Data Principal"** means the individual whose Personal Data is being processed or to whom the Personal Data relates.

H. **"Data Fiduciary"** means BITS Pilani, as the legal entity that, either independently or in collaboration with its campuses and divisions, determines the purposes and means of processing personal data across its physical campuses, digital platforms, and academic programmes.

I. **"Processor"** means any Institute or external service provider that processes Personal Data on behalf of BITS Pilani, the Data Fiduciary, without independently determining the purposes or means of such processing.

J. **"Child"** means an individual who has not completed the age of eighteen years, as defined under Section 2(f) of the Digital Personal Data Protection Act, 2023. In the context of BITS Pilani, this includes any applicant, student, or participant in academic or outreach programmes who is below the age of eighteen. In all matters where Personal Data of a Child is processed, appropriate safeguards shall be applied, and consent shall be obtained from the parent or lawful guardian as required under Section 9 of the DPDPA.

K. **"Consent"** means any freely given, specific, informed, and unambiguous indication of the Data Principal's agreement to the processing of their Personal Data for a specified purpose, either by a statement or by a clear affirmative action. In the case of a Child, consent must be provided by the parent or lawful guardian. Consent must be capable of being withdrawn at any time, and such withdrawal shall be as easy as giving consent.

L. **"Data Protection Officer"** means an individual appointed by BITS Pilani, where applicable, to oversee compliance with data protection obligations, coordinate responses to data breaches, and serve as a point of contact for Data Principals and regulatory authorities.

M. **"Digital Personal Data"** means Personal Data in digital form, including data collected, stored, or processed through online platforms, learning management systems, mobile applications, or other digital infrastructure operated by BITS Pilani.

N. "Consent Manager" means a person registered with the Data Protection Board of India under the DPDPA and the DPDP Rules, 2025, who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw their consent through an accessible, transparent, and interoperable platform.

O. "Data Protection Board" or "Board" means the Data Protection Board of India established under Section 18 of the DPDPA.

4. DATA PROCESSING PRINCIPLES

The Birla Institute of Technology and Science, Pilani, adheres to the following principles when processing Personal Data:

A. Lawfulness, Fairness, and Transparency

i. All such personnel & entities of BITS Pilani shall process Personal Data in a manner permitted under and for purposes that are not violative of any applicable laws.

ii. To the extent required by Applicable Laws, they shall ensure that a privacy impact assessment (PIA) and where necessary a data protection impact assessment (DPIA) is undertaken before commencing any activity that entails collection or processing of Personal Data.

iii. In jurisdictions where legitimate interests are a lawful ground for processing Personal Data under the Applicable Laws, whenever relying on it for a particular processing Pursuant to the principle of transparency, each BITS Pilani campus, its suppliers and service providers having access to Personal Data, shall ensure that it has a privacy notice published on their respective public-facing websites outlining, at a minimum, the following information:

1. the types of Personal Data collected or otherwise processed by it,
2. the purposes for which such Personal Data is used,
3. the types of parties with whom such Personal Data may be shared,
4. the rights available to the Data Principals with respect to their Personal Data, and
5. the manner in which the Data Principal can contact the Data Fiduciary to exercise their rights.
6. The manner in which the Data Principal may make a complaint to the supervisory or regulatory authority as provided in the Applicable Law.

iv. Grounds for processing under the DPDPA, the Institute only processes Digital Personal Data under two specific legal grounds:

1. Consent: When the Data Principal grants explicit permission as detailed under Section 6 of the DPDPA and Section 4(G)of this Policy.
2. Legitimate Uses: For specific lawful reasons permitted under Section 7 of the DPDPA. This includes voluntary data submission by the individual for a designated purpose, employment fulfillment for faculty and staff, legal mandates (such as court orders, judgments, or decrees), public health requirements, and medical emergencies.

B. Purpose Limitation

i. All such personnel & entities of BITS Pilani shall collect and process Personal Data only for specified, explicit, and legitimate purposes set out in the relevant privacy notice and not further process it in a manner that is incompatible with those purposes.

C. Data Minimization

i. All such personnel & entities of BITS Pilani shall ensure that the Personal Data processed by you is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is collected.
ii. All such personnel & entities of BITS Pilani will perform any assessments required under Applicable Laws before processing Sensitive Personal Data, and ensure that there is a clearly documented academic, administrative, or regulatory justification approved by the Institute or the relevant functional authority for the collection of such data. Moreover, Sensitive Personal Data shall only be collected where no reasonable alternative exists to fulfill the intended academic or institutional purpose.

D. Storage Limitation

i. All such personnel & entities of BITS Pilani may not retain the Personal Data for longer than is necessary to fulfil the purposes for which it was collected or otherwise processed unless there is a legal obligation to do so.
ii. Each BITS Pilani campus, its supplier and service providers having access to Personal Data, must have a data retention policy in place that includes the following attributes: identify in an itemized manner the purpose of retention (e.g. legal obligation, marketing based on consent, employment-related purposes, etc.) for each category of Personal Data.
1. clearly set out the timeline of retention period for each category of Personal Data.
2. contain details of how the Personal Data is to be disposed upon expiry of the retention period. Disposal methods may include deletion, purging, or irreversible anonymization, depending on the nature of the data and the risks associated with its retention;
3. outline the roles and responsibilities of internal and external stakeholders for ensuring compliance with the policy;
4. set out the frequency of review of the policy which shall be no less than once a year.

iii. The data retention schedule is set out in Appendix 1-A and legal/regulatory obligations for retaining data are set out in Appendix 1-B. BITS Pilani campuses are encouraged to refer to the minimum retention periods specified in Appendix 1-B and create their own maximum data retention schedule in the format set out in Appendix 1-A.
iv. Where there is a legal, regulatory, academic, or administrative obligation to retain Personal Data for a specified duration (e.g., student transcripts, employee service records, financial audit data), retention shall be limited to only those Personal Data attributes necessary to fulfill such obligations under the Applicable Law or institutional policy.
v. Where Personal Data forms part of larger databases that are required to be retained for analytics or other record-keeping requirements, you must ensure that the Personal Data is anonymized in a manner that reidentification is not possible.
vi. In accordance with the DPDP Rules, 2025, personal data, associated traffic data, and

logs specified thereunder shall be retained for a minimum period of one (1) year for purposes such as responding to lawful requests and supporting investigations, notwithstanding any shorter period specified in a campus-level retention schedule; upon expiry of the applicable retention period, such data shall be erased unless retention is required under any other law. Personal Data shall further be erased as soon as the purpose for which it was collected is no longer being served, including where consent has been withdrawn, subject to any legal obligation to retain it. It is recorded that the three-year erasure regime and 48-hour pre-erasure notification requirement under the Third Schedule of the DPDP Rules apply to specified classes of e-commerce entities, online gaming intermediaries, and social media intermediaries, and are not applicable to the Institute.

E. Integrity and Confidentiality

i. All such personnel & entities of BITS Pilani shall process Personal Data only in accordance with the Institute's policies with respect to appropriate technical and organizational measures to protect the Personal Data against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.

ii. Where Personal Data is used as a data input for any generative AI models, safeguards must be put in place such that the Personal Data is not used to train the model (unless prior written consent is taken from the Data Principals for the same), and the use is strictly in accordance with the applicable privacy laws . For this reason, one should not use any AI (Artificial Intelligence) tools similar to but not limited to ChatGPT, CoPilot etc., wherever personal data/sensitive/confidential data is involved, without explicit approval from the relevant Institute's information security team or the BITS Pilani IT team.

iii. All such personnel & entities of BITS Pilani shall not share Personal Data internally or externally, without establishing a strict need-to-know and in accordance with the Institute's policies on access control and use of third-party platforms. The Institute may deploy pseudonymization or data masking techniques before sharing data with third parties where access to Personal Data components is not essential for purposes of the engagement with the third party.

iv. Any third parties having access to Personal Data must mandatorily be required to sign an agreement (e.g., a Data Processing Agreement) outlining their obligations to protect the Personal Data from any unauthorized or unlawful use, access and disclosure. Where a standard set of clauses are prescribed under the Applicable Law (e.g. EU SCCs), such clauses must be executed in accordance with the Applicable Law.

v. Personal Data may not be shared with any Processor, without undertaking a third party privacy due diligence including an assessment of the technical controls enabled by the Processor.

vi. Suppliers, contractors, and service providers are strictly prohibited from sharing personal data collected or retained by BITS Pilani with any third party, including their own affiliates or subsidiaries. Exceptions are only permitted with prior, explicit written consent from the authorized BITS Pilani Campus.

F. Accuracy

i. Where Personal Data is used to make a decision that affects a Data Principal (including

decisions relating to admissions, evaluation, employment, payroll, benefits, discipline, or placements), or is disclosed to another Data Fiduciary, the Institute shall ensure the completeness, accuracy, and consistency of such Personal Data, in accordance with Section 8(3) of the DPDPA.

ii. Each BITS Pilani campus shall maintain reasonable mechanisms enabling Data Principals to have inaccurate or misleading Personal Data corrected, incomplete Personal Data completed, and outdated Personal Data updated, in accordance with Section 5 of this Policy.

G. Consent Management

All BITS Pilani campuses and their service providers shall ensure that:

1) When consent is being relied upon as a ground for processing under the Applicable Law, a request for taking consent must be accompanied by a notice to the Data Principal:
   i. in clear and plain language (i.e. not complex legal language), containing the information set out in section 4(a-iv) herein,
   ii. in an itemized (preferably in a tabular form) format setting out the description of the Personal Data against the purpose of processing and a description of the goods or services to be provided or the services to be enabled by such processing.
2) Data principals should be allowed to withdraw their consent at any time, with the manner of withdrawing consent being as easy as giving consent.
3) Records of consents and withdrawals, if any, must be maintained at least for a period of seven (7) years unless otherwise required to be purged under applicable laws.

5. DATA PRINCIPAL RIGHTS

Data Principals shall have the following rights with respect to their Personal Data, subject to certain exemptions as set out in the Applicable Laws. To the extent the Applicable Laws conflict with the Data Principal Rights enumerated in this section, the Institute will follow the approach that gives more rights to the Data Principal.

A. Right to Withdraw Consent.

i. Where processing of Personal Data is based on consent of the Data Principal, a technology enabled process must be operationalized to allow the Data Principal to withdraw their consent for specific processing activities.
ii. If processing of certain Personal Data attributes is essential for provision of the services being availed by the Data Principal, then the Data Principal must be informed that such services will not be available to them as a result of withdrawal of consent.

B. Right to Access. Where a Data Principal requests for access to their Personal Data, the following information should be provided to the Data Principal:

i. a summary of the Personal Data attributes processed by the Institute;

ii. a summary of the processing activities undertaken on such Personal Data;
iii. the credentials of other Data Fiduciaries and Processors with whom the Personal Data has been shared and a description of the Personal Data so shared; and
iv. and any other information that may be prescribed under the applicable law.

C. Right to Correct. The Data Principal also has the right to have their Personal Data corrected, completed or updated.

D. Right to Erase. The Data Principal may request to have their Personal Data, partly or completely, erased from the Institute's records. The following rules must be followed before erasing any Personal Data:

i. Personal Data cannot be erased where there is a legal obligation on the Institute to retain that data for a certain specified number of years under any other law for the time being in force.
ii. If Personal Data is essential for provision of services availed by the Data Principal, then the same must be informed to the Data Principal before erasure of such Personal Data.

E. Right to Grievance Redressal. Under the Digital Personal Data Protection Act, 2023 of India ("DPDPA"), the Data Principals also have the right to raise a grievance with the Institute related to the processing of their Personal Data. Once a Data Principal files a formal complaint with the Data Protection Board of India (DPB), the Institute (acting as the Data Fiduciary) is legally obligated to respond to the DPB's inquiries, provide necessary digital records, and implement any urgent remedial or mitigation orders issued by the Board. Conversely, the individual (acting as the Data Principal) holds the legal duty to cooperate with the inquiry by providing verifiably authentic information and must refrain from filing false or frivolous complaints.

a. There may be other rights available to Data Principals in different jurisdictions which must be adhered to. In case of any doubts, please refer to the relevant Institute's Legal team for more information.
b. Institute, its suppliers and service providers having access to Personal Data shall have a documented procedure in place for complying with requests received from Data Principals to exercise the rights available to them under the Applicable Laws.
c. You must follow the policies and procedures set out by the relevant BITS Pilani campus for responding to data principal rights requests.
d. Unless otherwise required under the Applicable Laws, each BITS Pilani campus and its service providers shall, at a minimum, comply with the following requirements:
i. Respond to and address any Data Principal request relating to the access,

correction, completion, updating, or erasure of Personal Data within a reasonable time and, in no event, later than ninety (90) days from the date of the request, in accordance with Rule 14(3) of the Digital Personal Data Protection Rules, 2025. If additional time is required due to the quantum of data or other operational challenges, the Data Principal should be notified of the same and informed of the revised timeline for completing the request; in no event shall the timeline extend beyond ninety (90) days from the date of the request.

ii. Outline in the Data Principal Request Management Policy, the manner in which the identity of the requestor will be verified. The Personal Data collected to verify the individual's identity must be commensurate with the type of request. (e.g. email OTP based authentication can be undertaken for students);
iii. Provide a mechanism for the Data Principals to exercise their rights through the campus's website and mobile application (where available);
iv. Mention in their Privacy Notice published on the website/app, the period within which it will resolve a grievance raised by the Data Principal, which period should not be greater than ninety (90) days or any other period prescribed by the law;
v. Publish on its website and app the particulars required to be furnished by the Data Principal in order to exercise their right to nominate one or more individuals to exercise the Data Principal's rights.
vi. If a Data Principal request is refused on certain grounds available under the law, the requestor must be notified of the same within thirty (30) days from date of request, along with the reasons for refusal.
vii. All Data Principal requests must be logged and a record maintained for at least one (1) year.

e. Where the request is received by the supplier, contractor or service provider of the Institute, it shall immediately, but no later than within twenty-four (24) hours of receipt of request, inform the Institute of the request and co-operate with the Institute to respond to the request.

6. DUTIES OF DATA PRINCIPALS.

In accordance with Section 15 of the DPDPA, every Data Principal shall, while exercising their rights under this Policy:

(a) comply with the provisions of all applicable laws;
(b) not impersonate another person while providing Personal Data for a specified purpose;
(c) not suppress any material information while providing Personal Data for any document, unique identifier, proof of identity, or proof of address issued by the

State or its instrumentalities;

(d) not register a false or frivolous grievance or complaint with the Institute or the Data Protection Board; and

(e) furnish only such information as is verifiably authentic while exercising the right to correction or erasure.

7. PROCESSING THE PERSONAL DATA OF CHILDREN AND PERSONS WITH DISABILITIES

A. Verifiable Parental Consent

Before processing any child's personal data, the Institute will obtain verifiable consent from their parent or legal guardian. This follows Section 9(1) of the DPDPA and Rule 10 of the DPDP Rules, 2025. We will verify the guardian's identity using:

i. Existing identity and age records held by the Institute.
ii. ID details voluntarily shared by the parent or guardian.
iii. Official digital tokens linked to government-authorized services (e.g., DigiLocker).
iv. Audit Trail: We will maintain records of consent, verification methods, dates, purposes, and guardian identities for accountability.

B. Persons with Disabilities

If a user is a person with a disability under a lawful guardianship, the Institute will obtain verifiable consent from their legal guardian. We will verify the guardian's legal appointment through court orders or designated disability law authorities according to Rule 11 of the DPDP Rules, 2025.

C. Prohibited Processing Activities

The Institute will not engage in tracking, behavioral monitoring, or targeted advertising directed at children. We strictly prohibit processing a child's personal data in any way that could harm their well-being, per Sections 9(2) and 9(3) of the DPDPA, unless allowed under Section 7(D)

D. Educational Institution Exemptions

As an educational institution, the Institute may utilize specific exemptions under Rule 12 and the Fourth Schedule of the DPDP Rules, 2025. These exemptions lift certain restrictions on parental consent and behavioral monitoring under strict conditions:

Scope: Data processing must be restricted strictly to core educational activities,

safety measures, or welfare actions (e.g., campus CCTV, attendance tracking, and school transport safety).
Restrictions: This exemption cannot be used for analytics, user profiling, marketing, or commercial gains.
Oversight: Any use of this exemption must be fully documented, kept strictly necessary and proportionate, and reviewed regularly by our Data Protection Officer.

E. General Policy Alignment

The rules in this section add to-and do not replace-our core privacy duties. The Institute remains fully bound by all standard obligations, including clear user notification, purpose limitation, data minimization, safe data retention, security safeguards, and data breach reporting.

8. CCTV AND VIDEO SURVEILLANCE, EVENTS, INSTITUTIONAL MEDIA ETC.

1. CCTV

A. Purpose and institutional framework. The Institute operates closed-circuit television (CCTV) surveillance systems across its campuses to provide for the safety and security of students, staff and visitors; to prevent and detect crime, theft, sabotage and harassment and to support investigations and, where required, prosecution; to protect Institute buildings, facilities and property; and to assist in risk management and in the resolution of incidents, claims and allegations. CCTV systems shall be implemented, operated and maintained in accordance with the Institute's CCTV Camera Standard Operating Procedure ("CCTV SOP"), which shall be read together with, and subject to, this Policy. In the event of any inconsistency between the CCTV SOP and this Policy in relation to the processing of Personal Data, this Policy shall prevail and the CCTV SOP shall be updated accordingly.

B. Personal Data and notice. CCTV footage in which an individual is identifiable constitutes Personal Data and shall be processed in accordance with the data processing principles set out in this Policy. Prominent signage shall be displayed at campus entry points and in monitored areas informing individuals that CCTV surveillance is in operation, and information regarding such surveillance shall be included in the Institute's privacy notices. CCTV shall not be installed in areas where individuals have a heightened expectation of privacy, including hostel rooms, washrooms, changing facilities and medical consultation rooms, and shall not be used for covert monitoring except where authorized under Applicable Law.

C. Governance and access control. The CCTV system shall be monitored only by the Chief Security Officer (CSO) and personnel authorized under the CCTV SOP,

with institutional oversight by the stakeholders identified therein (including the IPC Head, IT Manager, Dean Administration, CSO, EMU Chief, Chief Warden and Chief of SWD). Access to footage shall be restricted on a strict need-to-know basis. Requests by students to view footage shall follow the procedure prescribed in the CCTV SOP, including submission of the prescribed request form through the SWD office and authorization by the Chief Warden, with viewing conducted under supervision. Copies or extracts of recordings shall be released only upon written request to the Head IPC with due authorization of the Dean Administration. Disclosures to law enforcement or other authorities shall be made in accordance with Applicable Law, and all access to and disclosures of footage shall be logged.

D. Retention. In accordance with the CCTV SOP and the storage limitation principle of this Policy, CCTV footage shall be retained for a maximum of thirty (30) calendar days, after which it shall be securely deleted or overwritten. Where footage is required in connection with an incident, investigation, claim, disciplinary matter or legal proceeding, it may be retained specifically in that context until the matter is resolved, following which it shall be securely deleted. The retention entry for CCTV footage in Appendix I-A shall at all times correspond to the period specified in the CCTV SOP, and any revision to that period shall be made consistently in both documents, subject to any statutory retention requirement applicable to a particular campus.

E. Security of recordings. Recordings shall be stored on network video recorders located in the secured IPC server room, with backups of essential footage held in secured, lockable cabinets in the CCTV control room, and shall be protected by appropriate technical and organizational measures consistent with the Technical Measures section of this Policy.

F. Impact assessment and review. Any new deployment or material expansion of CCTV or other electronic surveillance (including biometric or access-control systems) shall be subject to Data Protection Impact Assessment oversight by the DPO in accordance with the Responsibilities section of this Policy, and the necessity and proportionality of camera coverage shall be reviewed periodically.

2. EVENT PHOTOGRAPHY, VIDEOGRAPHY AND INSTITUTIONAL MEDIA

A. Scope. This section governs the collection, use, storage and publication of photographs, video and audio recordings and live streams captured at Institute-level events, convocations and other ceremonial functions, student-driven cultural, sports and technical fests, academic activities, conferences, workshops

and other official programmes, whether captured by Institute personnel, photographers or videographers engaged by the Institute, student bodies authorized by the Institute, or accredited media. Such media in which an individual is identifiable constitute Personal Data and shall be processed in accordance with this Policy.

B. Notice and consent. Attendees and participants shall be informed in advance, through event notices, invitations, registration forms and/or prominent signage at the venue, that photography and recording will take place, of the purposes of such recording and of the channels on which the media may be published. Where registration is used, consent for event photography and publication shall, where practicable, be obtained at the time of registration. Reasonable measures, such as designated no-photography zones or the ability to notify organizers, shall be made available where feasible to individuals who do not wish to be photographed. Focused or close-up images of an identifiable individual intended for prominent use in promotional or marketing material shall require the specific consent of that individual.

C. Children. Identifiable images or recordings of Children shall be published only with the verifiable consent of the parent or lawful guardian in accordance with the provisions of this Policy on Children's Personal Data, save for incidental appearances in wide-angle or crowd imagery of public events. In no case shall a Child's image be published together with personal details such as name, programme or residence without such consent.

D. Use and publication. Event media shall be used only for legitimate institutional purposes, including publication on official Institute websites and social media channels, newsletters, annual reports, prospectuses, event documentation and institutional archives. Captions and tags shall be limited to the minimum necessary. Event media shall not be used in third-party commercial advertising, sold or licensed to third parties, or used in a manner that discloses Sensitive Personal Data or places an individual in a sensitive or misleading context, without the specific consent of the individuals concerned.

E. Engaged photographers and media. Photographers, videographers, streaming providers and similar service providers engaged by the Institute or by authorized student bodies shall be bound by written agreements consistent with the Integrity and Confidentiality provisions of this Policy, providing for purpose limitation, transfer of all original media to the Institute, secure deletion of media from the provider's own devices and systems within a defined period, and prohibition of any independent use, publication or portfolio use without the Institute's written approval and, where identifiable individuals are prominently featured, their consent. External media attending Institute events shall be subject to accreditation terms addressing the responsible use of recordings.

F. Storage, retention and Data Principal rights. Event media shall be stored in Institute-managed repositories with role-based access controls. Curated media forming part of the Institute's official record may be retained for archival purposes consistent with the storage limitation principle and applicable research and archival provisions. Any individual may request the review, removal or masking of media in which they are identifiable through the grievance mechanism set out in this Policy, and the Institute shall make reasonable efforts to remove or mask such media from platforms under its control, it being clarified that removal may not be feasible for media already lawfully distributed in print or by third parties.

9. RESPONSIBILITIES

A. Privacy representative.

i. The Institute shall appoint, at the institute level, a Data Protection Officer or privacy representative (hereinafter referred to as "DPO") Each BITS Pilani campus, its supplier and service providers having access to Personal Data shall designate a privacy representative to support the DPO in discharging the Institute's obligations under Applicable Laws at the campus level.

ii. The Institute shall publish the contact details of its DPO on its websites. in a prominent and easily accessible manner, and shall include the business contact information of the DPO (or of a person authorized to answer questions on the Institute's processing of Personal Data) in every response issued to a communication received from a Data Principal for the exercise of their rights.

iii. The suppliers and service providers having access to BITS Pilani Personal Data shall notify the relevant BITS Pilani campus of the identity and contact details of its DPO. The DPO shall,

a. Ensure that procedures for exercising Data Principal rights (such as access, correction, and grievance redressal) are in place and functioning effectively across all campuses and digital platforms;

b. Ensure that appropriate privacy notices and consent mechanisms are provided to Data Principals, including special provisions for obtaining verifiable parental or guardian consent when processing the Personal Data of Children, as defined under applicable law;

c. Ensure that clear and accessible information on Personal Data processing activities is made available to the public through privacy notices published on the Institute's website and other relevant platforms;

d. Advise on and oversee Data Protection Impact Assessments (DPIAs) for new academic, research, administrative, or infrastructure initiatives involving significant data processing, including the use of CCTV surveillance, biometric attendance systems, and digital access control;
e. Liaise with relevant supervisory or regulatory authorities in the event of a Personal Data Breach, and coordinate breach notification and mitigation efforts;
f. Maintain and regularly update the Personal Data inventory of the Institute, including data processed by academic departments, administrative offices, hostels, messes, and digital platforms such as WILP & BITS Digital;
g. Undertake training and awareness activities across the Institute to promote a culture of data protection among students, faculty, staff, and service providers;
h. Monitor compliance with data protection obligations specific to residential educational institutions, including those related to student accommodation, mess management, biometric systems, CCTV monitoring, and child data protection.

B. Process Owners.

Each BITS Pilani campus and division operates multiple academic, administrative, and operational processes that involve the processing of Personal Data. These include, but are not limited to, student admissions, academic records management, hostel and mess administration, faculty and staff recruitment, human resources operations, alumni engagement, research collaborations, guest house management, campus security systems (such as CCTV surveillance and biometric access), as well as health and wellness services provided through the medical center and any third-party wellness support vendors and agencies formally contracted by the Institute for the purpose of delivering health and wellbeing services.

HoDs/Unit Heads/ Division Heads & whoever is the in-charge officer of the respective function are responsible for ensuring that Personal Data within their respective domains is collected, processed, stored, and disposed of in compliance with this Policy and applicable data protection laws. They must also coordinate with the Data Protection Officer (DPO) to implement appropriate safeguards, especially when handling sensitive personal data such as medical records, biometric data, and child data, and respond to data-related requests or incidents.

1. The academic, administrative, or operational unit responsible for a particular Personal Data processing activity shall ensure that:
2. the processing activity is noted in the organization's personal data inventory;
3. any new Personal Data processing activity is submitted to the DPO for review;
4. any suspected or actual Personal Data Breach, is notified to the DPO immediately;

5. any information request or other notification received from a data protection authority or a supervisory authority, is notified to the DPO without delay;
6. not engage any third-party Processors without conducting due diligence to ensure that the third-party Processor can provide sufficient guarantees to comply with data protection laws and regulations; and
7. ensure all third parties with access to Personal Data enter into data processing agreements clearly setting out each party's role and responsibilities with respect to the Personal Data.
8. Suppliers and service providers processing BITS Pilani Personal Data shall provide to the relevant BITS Pilani Campus, documentation and/or other artifacts to demonstrate compliance with the requirements set out in sections 5(A)-(E).

10. TECHNICAL MEASURES

A. The Institute, its suppliers and service providers processing Personal Data shall ensure appropriate technical measures to protect the Personal Data from accidental or unauthorized access, alteration, use, processing, destruction or loss ("Personal Data Breach") including but not limited to the following or equivalent technical security measures:

a) encryption using AES 256 or higher encryption to be implemented for data at rest and in transit;
b) secure key management and key exchange controls to be deployed;
c) secure and ransomware protected backup to be implemented for protected data set;
d) pseudonymization needs to be enabled for personal data sets;
e) role based access-control to be enabled for access to personal data on the basis of the principle of least-privilege;
f) data-minimization controls to be enabled for reducing the amount of personal data collected and used;
g) putting in place a data breach response plan; and
h) implementing a data classification policy.

B. All BITS Pilani campuses shall comply with all Applicable Laws related to cybersecurity practices, data breach reporting, etc. including but not limited to the Cert-In requirements in India, where applicable.

C. All such personnel & entities of BITS Pilani shall comply with the policies put in place by the Institute for preventing Personal Data Breaches and notify the DPO immediately if they suspect or become aware of a Personal Data breach having occurred.

11. PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION

A. Upon becoming aware of any Personal Data Breach, the DPO, supported by the Institute's incident response team, shall without delay assess the nature, extent, timing, and location of occurrence of the breach, its likely impact, and the Data Principals affected. The seventy-two (72) hour reporting timeline under Rule 7 of the DPDP Rules, 2025 commences when the Institute becomes aware of the breach; the time of such awareness shall be documented.

B. Intimation to affected Data Principals. The Institute shall, without delay, intimate each affected Data Principal, in a concise, clear, and plain manner, through their user account or any registered mode of communication, providing: (a) a description of the breach, including its nature, extent, timing, and location of occurrence; (b) the likely consequences of the breach relevant to the Data Principal; (c) the measures implemented or proposed by the Institute to mitigate risk; (d) the safety measures the Data Principal may take to protect their interests; and (e) the business contact information of a person able to respond to queries on behalf of the Institute.

C. Intimation to the Data Protection Board. The Institute shall, without delay, inform the Data Protection Board of India of the breach, providing a description of its nature, extent, timing, location, and likely impact; and shall, within seventy-two (72) hours of becoming aware of the breach (or such longer period as the Board may permit on a written request), submit to the Board a detailed report covering: the broad facts relating to the breach and its causes; the measures implemented or proposed to mitigate risk; any findings regarding the person(s) responsible; remedial measures taken to prevent recurrence; and a report on the intimations issued to affected Data Principals.

D. Parallel statutory reporting. The obligations under this Section are in addition to, and shall be discharged in parallel with, the reporting of applicable cyber security incidents to the Indian Computer Emergency Response Team (CERT-In) within six (6) hours as required under the CERT-In Directions, 2022, and any other sectoral reporting obligations under Applicable Laws.

E. Processor breaches. Where a Personal Data Breach occurs at a Processor, supplier, contractor, or service provider processing Personal Data on behalf of the Institute, such entity shall notify the DPO without delay and in any event within twenty-four (24) hours of becoming aware of the breach, and shall extend full cooperation to the Institute in discharging its notification obligations; the notification obligations to the Board and to Data Principals shall remain with the Institute as the Data Fiduciary.

F. The Institute shall maintain a register of all Personal Data Breaches, including breaches not resulting in harm, together with the related assessments, notifications, and remediation records, and shall periodically test its breach response plan through simulation exercises.

12. CROSS-BORDER TRANSFER OF PERSONAL DATA

A. Pursuant to Section 16 of the DPDPA, the Institute reserves the right to transfer Personal Data outside the territory of India, except to any countries or territories restricted via notification by the Central Government. All such transfers are subject to specified regulatory conditions. The Data Protection Officer (DPO) shall monitor these restrictions to ensure that routine data flows—including transfers between Indian campuses and the Dubai campus, as well as transfers to international academic partners and service providers—remain strictly compliant with applicable laws.

B. All cross-border transfers shall be governed by appropriate contractual safeguards consistent with Section 4(E) of this Policy, and, where the personal data of individuals in other jurisdictions is involved, by the transfer mechanisms prescribed under the laws of those jurisdictions.

13. COMPLIANCE & ENFORCEMENT

Any violation of this Policy / Notice / Terms may result in appropriate action by BITS Pilani, depending on the nature and severity of the violation and the relationship with the Institute. Such action may include, without limitation, disciplinary proceedings under applicable institutional rules, suspension or termination of access to systems or services, termination of contractual arrangements, recovery of damages, and/or initiation of civil or criminal proceedings in accordance with applicable laws.

14. POLICY REVIEW

This Policy shall be reviewed once a year to ensure its continued relevance and compliance with applicable laws and regulations. The date of the latest update is set out on the last page of the Policy.

15. CONCLUSION

BITS Pilani, as an organization, is committed to protecting the privacy and security of Personal Data. By adhering to the principles and guidelines outlined in this Data Privacy Policy, we ensure that Personal Data is processed responsibly, transparently, and in accordance with the highest standards of data protection. For

any questions or concerns regarding this Policy, please reach out to the data protection officer of the Institute at compliance.cell@bits-pilani.ac.in

APPENDIX I-A
PERSONAL DATA RETENTION SCHEDULE

Sr. No.	Category of Personal Data	Timeline for Retention	Retention Purpose
1	Student academic records (admission, grades, transcripts)	Permanent	Academic history, verification, alumni services, legal and regulatory compliance
2	Student application data (applicants not admitted)	2–3 years	Admission analytics, future outreach, and audit trail
3	Student hostel and mess records	Duration of enrollment + 1 year	Residential services, grievance redressal, and audit
4	Medical and wellness records (Medical Center, third-party wellness support vendors and agencies)	7 years	Health services, legal compliance, and student welfare

5	Employee data (faculty/staff)	Duration of employment + 7 years	Employment related purposes, to protect the employer against loss or liability, to ensure employment history is maintained in case of future re-appointment, to provide employment related benefits incl. retirement benefits, legal compliance
6	Employee payroll and tax records	8 years	Statutory compliance and audit
7	Employee PF and gratuity records	7 years from date of payment	Legal obligation and dispute resolution
8	CCTV footage	1 month	Campus safety, incident

a

			investigation, and security monitoring
9	Biometric access logs	1 year	Access control, attendance, and security
10	Email & digital communication logs (e.g., Gmail, MS Teams)	3 years	ensuring security and traceability of data, , dispute resolution, maintaining confidentiality preventing unauthorized or unlawful use of BITS Pilani's confidential information, computer networks/systems
11	Visitor and guest house records	6 months	Campus security and guest management
12	Vendor and service provider data	10 years	Contractual and financial law compliance
13	Consent and withdrawal records	7 years	Legal audit trail and compliance with DPDPA 2023
14	Research participant data	As per research ethics guidelines or project duration + 5 years	Academic integrity, reproducibility, and compliance with funding agency requirements
15	Curated or processed event photography, videography and institutional media	Permanent	Student welfare, Promotion, public relations purposes .
16	Security, access, and system logs and associated traffic data (all systems)	Minimum 1 year	Compliance with the DPDP Rules, 2025 and CERT-In directions; responding to lawful requests and supporting

			investigations

APPENDIX I-B

Legal/Regulatory obligations to retain data

Sr. No.	Law/Regulation	Minimum retention period	Type of Data	Applicability
1	Companies Act, 2013	8 years	Books of accounts	Institute
2	Companies Act, 2013	8 years	Copies of all annual returns prepared under section 92 and copies of all certificates and documents	Institute
3	Companies Act, 2013	15 years	Register and index of debenture holders	Institute
4	Companies Act, 2013	Permanent	Minutes of Meetings, statutory registers, incorporation documents, share certificates and transfer forms, private placement records	Institute
5	Companies Act, 2013	8 years post satisfaction	Copies of instruments creating, modifying, or satisfying a charge	Institute
6	Minimum Wages Act, 1948 and The Code on Wages, 2019	3 years	Registers and records, wage slips, inspection books	Institute
7	Provident Fund and Miscellaneous Provisions Act, 1952 and The Code on Social Security, 2020.	10 years, The retention period shall be calculated from the date of	Records related to provident fund contributions	Institute .

Sr. No.	Law/Regulation	Minimum retention period	Type of Data	Applicability
		separation of the employee from the Institute, whether by resignation, retirement, death, or otherwise.		
8	Cert-In Guidelines 2022	180 days	Logs of all information communications technology (ICT) systems	Service providers, intermediaries, data centres, body corporates
9	Information Technology (Intermediaries Guidelines) Rules, 2011	180 days	Records of user data and communications	Intermediaries
10	Prevention of Money Laundering Act, 2002	5 years	Financial transactions, customer identification records, suspicious reports	Banks, financial institutions and reporting campuses
11	Foreign Exchange Management Act, 1999 and Foreign Contribution (Regulation) Act, 2010 (FCRA)	5 years	Records of foreign exchange transactions	Campuses involved in foreign exchange transactions or receiving foreign contributions/donations
12	Electronic Health Records (EHR) Standards, 2016 , (general clinical records)	3 years from date of last entry	All types of electronic health records, including patient history, diagnosis, treatment plans, prescriptions, and other relevant medical information	Medical Doctor or institution
13	Electronic Health Records (EHR) Standards, 2016 (medico-legal	Permanent	Records related to medico-legal cases, including injury reports, forensic reports, and	Medical Doctor or institution

Sr. No.	Law/Regulation	Minimum retention period	Type of Data	Applicability
	records)		other legal documentation	
14	Electronic Health Records (EHR) Standards, 2016 (minors' records)	Until age 18 plus 3 years	Records of minors	Medical Doctor or institution
15	Digital Personal Data Protection Rules, 2025 (Rule 6 read with Rule 8)	Minimum 1 year	Personal data, associated traffic data, and logs specified under the DPDP Rules, for responding to lawful requests and supporting investigations	All Data Fiduciaries

The retention periods mentioned below for medical and wellness records are applicable to educational institutions with healthcare facilities, such as BITS Pilani, and are aligned with general medical practice and institutional policy. While the Medical Council of India (MCI) Act, 1956, National Medical Commission (NMC) Act, 2019 and related regulations do not prescribe specific retention durations, the timelines provided are suggestive and based on standard healthcare documentation practices and legal prudence.

Type of Record	**Retention Period**	**Details**	**Source/Guideline**
Patient Medical Records	7 years from the separation of the employee/student from the Institute, or from any change in dependent status, as applicable	Includes patient history, diagnosis, treatment plans, prescriptions	General medical practice standards, state regulations
Inpatient Records	10 years from the date of discharge	Admission details, treatment during hospital stay, discharge summaries	General medical practice standards, state regulations
Outpatient Records	5 years from the last visit	Records of outpatient visits and follow-up care	General medical practice standards, state regulations
Surgical and Procedure Records	10 years from the date of procedure	Pre-operative and post-operative notes, consent forms, operative reports	General medical practice standards, state regulations
Laboratory and Diagnostic Test Reports	3 to 5 years from the date of test	Blood tests, imaging studies, biopsies, other diagnostic tests	General medical practice standards, state regulations
Consent Forms	10 years from the date of procedure	Signed consent forms for surgeries, treatments, and other medical procedures	General medical practice standards, state regulations
Birth and Death Records	Permanently	Records of births and deaths, including certificates	General medical practice standards, state regulations
Medico-Legal Records	Permanently	Records related to medico-legal cases, injury reports, forensic reports	General medical practice standards, state regulations

Revision History

Document Name : Birla Institute of Technology and Science, Pilani - Data Privacy Policy

Version Control	Date	Revision Made By:
V1.0_2025		
V2.0_2026	14-Jul-2026	Legal & Compliance Cell, (revised as per DPDP Act 2023 with its DPDP 2025 rules and other international privacy frameworks)