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.

3. DEFINITIONS

3.1 **"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.

3.2 **"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, and Mumbai, 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.

3.3 "**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**").

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

3.5 "**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.)

3.6 **"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.

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

3.8 **"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.

3.9 **"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.

3.10 **"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.

3.11 **"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.

3.12 **"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.

3.13 **"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.

4. DATA PROCESSING PRINCIPLES

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

4.1 Lawfulness, Fairness, and Transparency

4.1.1 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.

4.1.2 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.

4.1.3 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

activity, BITS Pilani shall ensure that a legitimate interest impact assessment (LIA) has been carried out to balance the interests and fundamental rights of the Data Principals against the legitimate interest pursued by the Data Fiduciary.

4.1.4 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:

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

4.2 Purpose Limitation

4.2.1 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.

4.3 Data Minimization

4.3.1 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.

4.3.2 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.

4.4 Storage Limitation

4.4.1 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.

4.4.2 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:

a) 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.

b) clearly set out the timeline of retention period for each category of Personal Data.
c) 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;
d) outline the roles and responsibilities of internal and external stakeholders for ensuring compliance with the policy;
e) set out the frequency of review of the policy which shall be no less than once a year.

4.4.3 A sample 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.

4.4.4 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.

4.4.5 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.

4.5 Integrity and Confidentiality

4.5.1 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.

4.5.2 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.

4.5.3 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.

4.5.4 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.

4.5.5 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.

4.5.6 Suppliers, contractors and service providers may not share the personal data collected/retained by BITS Pilani with any third party, including its affiliates or subsidiaries, unless otherwise agreed in writing by the relevant BITS Pilani Campus.

5. CONSENT MANAGEMENT

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

5.1 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:

5.1.1 in clear and plain language (i.e. not complex legal language),

5.1.2 containing the information set out in section 4.1.4 herein,

5.1.3 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.

5.2 Data principals should be allowed to withdraw their consent at any time, with the manner of withdrawing consent being as easy as giving consent. (e.g. if consent is taken through the mobile app, then withdrawal should also be through the same app).

5.3 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.

6. DATA PRINCIPAL RIGHTS

6.1 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.

6.1.1 **Right to Withdraw Consent.**

a) 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.

b) 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.

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

a) a summary of the Personal Data attributes processed by the Institute;
b) a summary of the processing activities undertaken on such Personal Data;
c) 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
d) and any other information that may be prescribed under the applicable law.

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

6.1.4 **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:

a) 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.
b) 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.

6.1.5 **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.

For BITS Pilani campuses operating in other jurisdictions, a documented process of grievance redressal can be put in place as a best practice as it encourages resolution of grievances before being referred to the supervisory/regulatory authorities.

6.2 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.

6.3 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.

6.4 You must follow the policies and procedures set out by the relevant BITS Pilani campus for responding to data principal rights requests.

6.5 Unless otherwise required under the Applicable Laws, each BITS Pilani campus and its service

providers shall, at a minimum, comply with the following requirements:

6.5.1 Respond to any Data Principal request within thirty (30) days from the date of request. 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 be extended beyond sixty (60) days from the date of the request.

6.5.2 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);

6.5.3 Provide a mechanism for the Data Principals to exercise their rights through the campus's website and mobile application (where available);

6.5.4 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 thirty (30) days or any other period prescribed by the law;

6.5.5 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.

6.5.6 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.

6.5.7 All Data Principal requests must be logged and a record maintained for at least three (3) years.

6.6 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.

7. RESPONSIBILITIES

7.1 Privacy representative.

7.1.1 Each BITS Pilani campus, its supplier and service providers having access to Personal Data shall appoint a data protection officer or a privacy representative (hereinafter referred to as "DPO")

7.1.2 The Institute shall publish the contact details of its DPO on its websites.

7.1.3 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.

7.1.4 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.

7.2 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 Mpower.

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.

7.2.1 The academic, administrative, or operational unit responsible for a particular Personal Data processing activity shall ensure that:

a) the processing activity is noted in the organization's personal data inventory;
b) any new Personal Data processing activity is submitted to the DPO for review;
c) any suspected or actual Personal Data Breach, is notified to the DPO immediately;
d) any information request or other notification received from a data protection authority or a supervisory authority, is notified to the DPO without delay;
e) 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
f) 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.

7.2.2 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 6.1 & 6.5.

8. TECHNICAL MEASURES

8.1 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.

8.2 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.

8.3 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.

9. 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.

10.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.

11.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 Registrar/ Deputy Registrar of the Institute at registrar@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, Mpower)	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 to 3 months	Campus safety, incident

			investigation, and security monitoring
9	Biometric access logs	6 months	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

APPENDIX I-B

Legal/Regulatory obligations to retain data

Sr. No.	Law/ Regulation	Minimum retention period	Type of Data	Applicability
1	Income Tax Act, 1961	6 years from end of assessment year	Tax returns, financial records, books of accounts	Any person filing tax return
2	Goods and Services Act, 2017	6 years	GST invoices, returns, and records	Any person filing tax return
3	Companies Act, 2013	8 years	Books of accounts	Company
4		8 years	Copies of all annual returns prepared under section 92 and copies of all certificates and documents	
5		15 years	Register and index of debenture holders.	
6		Permanent	Minutes of Meetings, statutory registers, incorporation documents, share certificates and transfer forms, private placement records	
7		8 years post satisfaction	Copies of instruments creating, modifying, or satisfying a charge	
8	SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015	8 years	All disclosures made to the stock exchanges incl. financial statements, annual reports, and other disclosures required under the listing agreement.	Listed campuses
9	Minimum Wages Act, 1948	3 years	Registers and records, wage slips, inspection books	All employers

10	Provident Fund and Miscellaneous Provisions Act, 1952	10 years	Records related to provident fund contributions	All establishments employing 20 or more persons or factories listed in Schedule 1
11	Employee State Insurance Act, 1948	5 years	Records related to employee state insurance contributions	All employers

12	Cert- In Guidelines 2022	180 days	Logs of all information communications technology (ICT) systems	Service providers, intermediaries, data centres, body corporates
13				
14	Information Technology (Intermediaries Guidelines) Rules, 2011	180 days	Records of user data and communications	Intermediaries
15	Prevention of Money Laundering Act, 2002	5 years	Financial transactions, customer identification records, suspicious reports	Banks, financial institutions and reporting campuses
16			s	
17	Foreign Exchange Management Act, 1999	5 years	Records of foreign exchange transactions	Campuses involved in foreign exchange transactions

18	Electronic Health Records (EHR) Standards, 2016	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
19		Permanent	Records related to medico-legal cases, including injury reports, forensic reports, and other legal documentation	
20		Until age 18 plus 3 years	Records of minors	

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 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	3 to 5 years from the last entry	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

BITS Pilani Personal Data Retention Schedule

Category of Personal Data	Retention Period	Applicable Law/Regulation
Student academic records (admission, grades, transcripts)	Permanent	UGC Guidelines, Institutional Policy
Student application data (applicants not admitted)	2–3 years	Institutional Policy
Student hostel and mess records	Duration of enrollment + 1 year	Institutional Policy
Medical and wellness records (Medical Center, Mpower)	7 years	Medical Council of India, Institutional Policy
Employee data (faculty/staff)	Duration of employment + 7 years	Income Tax Act, 1961; Institutional Policy
Employee payroll and tax records	8 years	Income Tax Act, 1961
Employee PF and gratuity records	7 years from date of payment	Employees' Provident Funds and Miscellaneous Provisions Act, 1952
CCTV footage	6 months	Institutional Policy
Biometric access logs	1 year	Institutional Policy
Email & digital communication logs (e.g., LMS, MS Teams)	3 years	Institutional Policy
Visitor and guest house records	6 months	Institutional Policy
Vendor and service provider data	10 years	Contractual and Financial Compliance
Consent and withdrawal records	7 years	Digital Personal Data Protection Act, 2023
Research participant data	As per research ethics guidelines or project duration + 5 years	Institutional Policy, Funding Agency Requirements

Revision History

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

Version Control	Date	Revision Made By:
V1.0_2025		