Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

DATA PROTECTION AND PRIVACY POLICY 2025

www.cutm.ac.in

Version 2

DATA PROTECTION AND PRIVACY POLICY 2025

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT
ODISHA

FOREWORD

At Centurion University of Technology and Management (CUTM), we recognize that data is one of the most valuable assets in the modern educational landscape. As an institution committed to academic excellence, innovation and responsible governance, we acknowledge our responsibility to protect the privacy, confidentiality and security of the personal and institutional information entrusted to us by students, faculty, staff, alumni, research collaborators and other stakeholders.

The Data Protection and Privacy Policy reflects our unwavering commitment to ensuring that all personal data is collected, processed, stored, shared and disposed of in a lawful, ethical, transparent and secure manner. In an era of rapid digital transformation, the responsible management of information is essential not only for regulatory compliance but also for maintaining trust, accountability and institutional integrity.

This policy establishes a comprehensive framework for safeguarding data and protecting the privacy rights of individuals while supporting the University's academic, research, administrative and outreach activities. It promotes a culture of data responsibility and reinforces the principles of transparency, confidentiality, fairness and security in all data-related practices across the University.

Through this policy, CUTM seeks to align its operations with national and international best practices in data protection and privacy management. It further strengthens our commitment to creating a secure digital environment that supports innovation, collaboration and informed decision-making while respecting the rights and expectations of all members of our community.

I encourage every member of the Centurion fraternity to understand and uphold the principles outlined in this policy. Together, let us foster a culture of trust, responsibility and digital ethics that safeguards information and supports the University's vision of excellence and sustainable growth.

Prof. (Dr.) Supriya Pattanayak
Vice Chancellor
Centurion University of Technology and Management

Contents

Data Protection and Privacy Policy

1. Purpose

Centurion University of Technology and Management is committed to protecting the privacy and personal data of all individuals with whom it interacts, including students, staff, research participants, alumni, partners and visitors. This commitment is grounded in the Digital Personal Data Protection Act, 2023 ("DPDPA"), the Information Technology Act, 2000 ("IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), together referred to as "Data Protection Laws."

The university recognises that responsible, lawful and transparent handling of Personal Data is essential to maintaining the trust of its stakeholders, preserving its institutional integrity and fulfilling its obligations as a multi-campus university operating across Odisha and other states of India. This policy sets out the University's approach, principles, responsibilities and procedures for the collection, processing, storage and disposal of Personal Data.

2. Scope

This policy applies to all Processing of Personal Data carried out by or on behalf of CUTM, including:

- All academic and administrative staff employed across all CUTM campuses
- Students enrolled in any programme at CUTM
- Research scholars, post-doctoral fellows and academic visitors
- Contractual staff, consultants and third-party service providers who access Personal Data on behalf of CUTM
- Affiliates, partner institutions and agents who process Personal Data in connection with CUTM activities

This policy also applies to off-campus Processing of Personal Data, including remote work, fieldwork, collaborative research and any digital processing through CUTM-authorised systems. Processing Personal Data off-campus presents heightened risks of loss, theft or unauthorised disclosure; staff and students must apply the same rigour as on campus.

3. Policy Statement

- This policy does not constitute a term of employment or enrolment, but compliance with it is a condition of continued association with the University. Employees are required to familiarise themselves with and act in accordance with this policy at all times.
- Any failure to comply with this policy may result in disciplinary action under applicable service rules or student disciplinary codes. Third parties and contractors who fail to comply may have their access to CUTM data systems restricted or terminated.
- CUTM may supplement this policy with additional procedures, guidelines or circulars issued from time to time. Such supplementary instruments shall be read as part of this policy.

4. Background

- The Digital Personal Data Protection Act, 2023 (DPDPA) governs the processing of digital personal data of individuals ("Data Principals") in India. It establishes the rights of Data Principals and the obligations of Data Fiduciaries — entities that determine the purpose and means of processing personal data. CUTM acts as a Data Fiduciary in respect of the personal data it processes.
- The SPDI Rules under the IT Act prescribe reasonable security practices for handling sensitive personal data, including financial information, health data, biometric information and passwords. CUTM is bound by these requirements in its operations.
- Non-compliance with Data Protection Laws can lead to:
    i. Financial penalties imposed by the Data Protection Board of India under the DPDPA (which may extend to significant sums depending on the nature and gravity of the breach)
    ii. Civil liability to individuals harmed by a data breach or unlawful processing
    iii. Reputational damage adversely affecting student admissions, research partnerships and institutional rankings
- CUTM's obligations under the DPDPA include: processing data only for lawful purposes; obtaining free, specific and informed consent where required; maintaining accuracy of data; implementing security safeguards; enabling Data Principal rights; and notifying breaches to the Data Protection Board of India and affected individuals.

5. Data Protection Definitions

The following key terms are used throughout this policy and should be interpreted in the context of applicable Data Protection Laws:

Term	Meaning
Data Principal	The individual to whom Personal Data relates. In the CUTM context, this includes students, staff, research participants, alumni and other natural persons whose data CUTM holds or processes.
Data Fiduciary	An entity that determines the purpose and means of processing Personal Data. CUTM is the Data Fiduciary for the majority of Personal Data processed in connection with its academic and administrative operations.
Data Processor	An entity that processes Personal Data on behalf of a Data Fiduciary. Third-party vendors, IT service providers and partner institutions acting under contract may be Data Processors to CUTM.
Personal Data	Any data about an individual that identifies or can identify that person, directly or in combination with other data. Includes name, date of birth, student/employee ID, contact details, photographs, academic records and location data.
Sensitive Personal Data (SPDI)	Personal Data classified as sensitive under the SPDI Rules 2011: passwords, financial information, physical or mental health data, sexual orientation, biometric data, medical records and similar categories. Requires a higher standard of protection.
Processing	Any operation or set of operations performed on Personal Data, including collection, recording, storage, retrieval, use, disclosure, transfer and deletion — whether or not by automated means.
Consent	A freely given, specific, informed and unambiguous indication of the Data Principal's agreement to the processing of their Personal Data for a stated purpose. Consent must be capable of being withdrawn at any time.
Data Breach	Any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, Personal Data transmitted, stored or otherwise processed by or on behalf of CUTM.
DPDPA	Digital Personal Data Protection Act, 2023 — the primary legislation governing personal data protection in India.
SPDI Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

6. Responsibilities under Data Protection Laws

- CUTM, as a Data Fiduciary, bears overall accountability for compliance with Data Protection Laws in respect of all Personal Data processed in connection with its functions.
- The Vice-Chancellor holds ultimate institutional responsibility for this policy. The Registrar is designated as the senior officer responsible for data protection governance at CUTM.
- CUTM shall designate a Data Protection Officer (DPO) who shall be responsible for day-to-day oversight of data protection compliance, handling Data Principal requests and grievances, coordinating breach notifications and conducting training and awareness activities. The DPO can be contacted at dataprotection@cutm.ac.in.
- A Data Governance Committee (DGC) shall be established comprising the DPO, the Chief Information Officer (or equivalent), the Registrar and representatives of major Schools and Services. The DGC shall define, approve and monitor the University's information governance framework, including data protection policies, procedures and compliance activities.
- Deans, Directors, Heads of Departments and Heads of Service are responsible for ensuring that all Personal Data processed within their respective units is handled in compliance with this policy and applicable Data Protection Laws.
- Each School or Service shall designate a Data Protection Champion (DPC) who shall serve as the first point of contact for data protection matters within that unit, raise awareness and liaise with the DPO. DPCs are supported by the central Data Governance Committee.
- All staff shall be responsible for:

    i. Completing CUTM-provided data protection training on joining and at regular intervals thereafter
    ii. Ensuring that Personal Data processed by them is handled in accordance with this policy and applicable law
    iii. Keeping their own personnel information accurate and informing HR of any changes
    iv. Reporting actual or suspected data breaches or policy violations immediately to their DPC or the DPO

- Staff supervising students who process Personal Data as part of coursework, projects or placements shall ensure that such students are informed of their obligations under this policy and applicable Data Protection Laws.
- Students processing Personal Data as part of academic research or projects must seek ethical clearance through the relevant School's Research Ethics Committee and shall be bound by this policy.
- Third-party contractors and service providers who process Personal Data on behalf of CUTM shall be required by contract to comply with the provisions of this policy and applicable Data Protection Laws. CUTM remains responsible as Data Fiduciary for data processed by such parties.

7. Data Protection Principles

CUTM shall process Personal Data in accordance with the following principles, which reflect the requirements of the DPDPA and SPDI Rules:

- **Lawful Purpose:** Personal Data shall only be collected for a lawful purpose, whether pursuant to a legal obligation, a contract, the performance of a function in the public interest or with the free, specific and informed consent of the Data Principal.
- **Purpose Limitation:** Personal Data shall be collected only for specified, explicit and legitimate purposes and shall not be processed in a manner incompatible with those purposes. Data obtained for one purpose shall not be used for an unrelated purpose without the Data Principal's further consent.
- **Data Minimisation:** Only Personal Data that is adequate, relevant and necessary for the stated purpose shall be collected. Excessive data shall not be retained; if data is inadvertently collected that exceeds necessity, it shall be deleted promptly.
- **Accuracy:** CUTM shall ensure that Personal Data it holds is accurate and up-to-date. Where inaccurate data is identified, it shall be corrected or deleted without delay. Staff, students and other individuals are encouraged to notify CUTM of any changes to their personal information.
- **Storage Limitation:** Personal Data shall not be retained for longer than is necessary for the purpose for which it was collected. CUTM's Retention and Disposal Schedule (see Section 14) governs the retention periods applicable to different categories of data.

- **Security:** Appropriate technical and organisational measures shall be implemented to protect Personal Data against unauthorised or unlawful processing, accidental loss, destruction or damage (see Section 8).
- **Accountability:** CUTM shall be able to demonstrate compliance with this policy and the Data Protection Laws. It shall maintain records of processing activities, implement Privacy by Design and conduct Data Protection Impact Assessments (see Section 20) where appropriate.
- **Transparency:** Data Principals shall be informed of how, why and on what legal basis their Personal Data is being processed. CUTM shall publish privacy notices for students, staff, alumni, research participants and visitors.

CUTM shall generally not process Personal Data unless one of the following lawful bases applies:

- Performance of a contract with the individual (e.g., student enrolment, employment contract)
- Compliance with a legal obligation imposed on CUTM
- Performance of a function in the public interest or in the exercise of official authority
- Legitimate interests of CUTM that are not overridden by the rights and freedoms of the Data Principal
- Consent provided freely and specifically by the Data Principal for a stated purpose

8. Policy Ownership

Under the DPDPA 2023 and other applicable Data Protection Laws, individuals whose data is held by CUTM have the following rights:

- **Right to Access:** Data Principals may request a summary of the Personal Data held about them and information regarding the processing activities to which it is subject. Requests should be submitted in writing to the DPO. CUTM shall respond within 30 days of receipt of a valid request.
- **Right to Correction and Erasure:** Data Principals may request correction of inaccurate or incomplete Personal Data or erasure of data that is no longer necessary for the purpose for which it was collected or where consent has been withdrawn. Requests shall be processed within 30 days.

- **Right to Grievance Redressal:** Data Principals may lodge a grievance with CUTM's designated DPO. If the grievance is not resolved to the individual's satisfaction within the prescribed period, the individual may escalate the matter to the Data Protection Board of India established under the DPDPA.
- **Right to Withdraw Consent:** Where CUTM processes Personal Data on the basis of consent, the Data Principal may withdraw consent at any time. Withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.
- **Right to Nominate:** Data Principals may nominate another individual to exercise their rights in the event of death or incapacity, in accordance with DPDPA provisions.
- **Protection of Children's Data:** Where CUTM processes Personal Data of children (individuals under the age of 18), it shall obtain verifiable consent from a parent or guardian and shall not process such data in a manner that is likely to cause harm to the child. CUTM shall not engage in tracking, behavioural monitoring or targeted advertising in respect of children's data.

CUTM shall publish procedures for the exercise of these rights on its institutional website and intranet portal. Staff receiving Data Principal rights requests shall immediately forward them to the DPO.

9. Sensitive Personal Data and Special Categories

- Sensitive Personal Data or Information (SPDI) — as defined under the SPDI Rules 2011 — includes passwords, financial data, physical and mental health information, sexual orientation, biometric information, medical records and caste or tribe information where collected. CUTM shall handle SPDI with the highest standard of care.
- Processing of SPDI shall require the explicit, informed and written consent of the Data Principal, unless processing is necessary for compliance with a legal obligation or an order of a court or tribunal. Consent forms shall clearly describe the data being collected, the purpose and intended disclosures.
- SPDI shall not be collected unless necessary for a legitimate institutional purpose and shall be kept for only as long as necessary. Access to SPDI shall be restricted on a strict need-to-know basis.

- CUTM shall not transfer SPDI to any third party without prior consent of the Data Principal, except where required by law or court order. Any third party to whom SPDI is transferred must maintain the same level of protection as CUTM.
- Staff wishing to process SPDI for any purpose must consult the DPO before collection or processing commences.

10. Security of Data

- CUTM shall implement and maintain reasonable security practices and procedures as required under the SPDI Rules, including technical, administrative and physical safeguards appropriate to the sensitivity and volume of data processed.
- All Personal Data shall be accessible only to those individuals who require it to perform their institutional duties. Access controls shall be implemented and reviewed regularly. The following minimum standards apply:

  i. Physical records containing Personal Data must be stored in lockable rooms or filing cabinets with controlled access
  ii. Computerised Personal Data must be password-protected; strong passwords must be used and changed periodically
  iii. Multi-factor authentication shall be implemented for systems containing Sensitive Personal Data

- Personal Data must not be stored on unencrypted removable media (USB drives, external hard disks, CDs, DVDs) or personal mobile devices unless encrypted. Backup copies shall be maintained on CUTM's secure institutional servers. Data must not be stored on personal cloud services (e.g., personal Google Drive, Dropbox) without authorisation.
- Particular care shall be taken when transmitting Personal Data by email or other electronic channels. Staff must use CUTM institutional email accounts for official communications involving Personal Data and must not use personal email accounts for this purpose.
- PC and terminal screens displaying Personal Data shall be positioned to prevent unauthorised viewing. Screen locks shall activate automatically after a period of inactivity. Physical records shall not be left unattended where they can be accessed by unauthorised persons.

- Personal Data shall be securely deleted or disposed of when no longer required. Electronic records shall be wiped using secure deletion tools; physical records shall be shredded or disposed of as confidential waste. Hard drives and storage media from decommissioned equipment shall be securely destroyed.
- Where CUTM engages external organisations (Data Processors) to process Personal Data on its behalf, appropriate data processing agreements shall be executed prior to any data sharing. Such agreements shall impose obligations of confidentiality, security and compliance equivalent to those applicable to CUTM.
- CUTM shall conduct periodic information security audits and vulnerability assessments to evaluate the effectiveness of its security measures.

11. Reporting Data Breaches

- Any member of staff, student or contractor who becomes aware of an actual or suspected data breach or of any event that may have compromised the security, integrity or confidentiality of Personal Data, must report it immediately to the DPO at dataprotection@cutm.ac.in.
- In accordance with the DPDPA 2023, CUTM shall notify the Data Protection Board of India and affected Data Principals of any personal data breach in the prescribed form and within the timeframe specified by the Board's regulations.
- On receipt of a breach report, the DPO shall:

  i. Assess the nature, scope and impact of the breach
  ii. Initiate containment and remedial measures without delay
  iii. Determine notification obligations and, where required, notify the Data Protection Board and affected Data Principals
  iv. Document the breach and the steps taken in the University's Breach Register
  v. Conduct a post-incident review to prevent recurrence

- Staff or students who knowingly delay reporting a breach or who conceal or facilitate a breach, may be subject to disciplinary proceedings.
- Where CUTM is acting as a Data Processor on behalf of a third party, it shall notify that party of any breach affecting their data promptly and in accordance with the contractual terms agreed.

12. Acting as a Data Processor

- In the majority of its data processing activities, CUTM acts as a Data Fiduciary. However, in limited circumstances — such as when processing personal data on behalf of a government body, sponsoring organisation or research funding agency — CUTM may act as a Data Processor.
- Staff who are uncertain whether CUTM is acting as Data Fiduciary or Data Processor in a given context shall consult their DPC or the DPO. It is essential to correctly identify this relationship before processing commences.
- Where CUTM acts as a Data Processor, its obligations (including security measures, breach notification and sub-processing arrangements) shall be governed by the data processing agreement with the Data Fiduciary, which must comply with applicable Data Protection Laws.

13. Accuracy, Adequacy, relevance and Proportionality

- CUTM shall take reasonable steps to ensure that all Personal Data held by it is accurate, adequate, relevant and proportionate to the purpose for which it was collected.
- Data Principals may request correction of inaccurate Personal Data at any time. If a staff member receives such a request but disputes the alleged inaccuracy, they shall record the dispute and refer the matter to the DPO.
- Staff should update their personal details through the HR management system (MyHR or equivalent). Students should update their details through the Student Information System or the Office of the Registrar. CUTM shall act promptly on notifications of changed circumstances.

14. Rights of Access to Personal Data

- Data Principals have the right to request access to the Personal Data held about them by the university. Such requests ("Data Access Requests") must be made in writing (including by email) to the DPO. CUTM shall respond within 30 days of receipt of a valid request.
- The university may decline to provide access to certain data in the limited circumstances permitted by Data Protection Laws (e.g., where disclosure would

prejudice a legal proceeding or where the data relates to third parties whose privacy cannot be adequately protected).

- Where a student requests access to examination scripts or assessments, scripts shall be made available for review in the presence of a representative from the Office of the Controller of Examinations. Examiner annotations and comments may be provided in transcribed form.
- CUTM shall maintain robust records management practices to enable efficient processing of Data Access Requests. Refer to the CUTM Records Management Policy for further guidance.

15. Disclosure of Personal Data

- Personal Data shall not be disclosed to any unauthorised party, including family members, media organisations, political bodies or law enforcement agencies, except in the circumstances described in this section.
- Personal Data may be legitimately disclosed where:

  i. The disclosure is in the legitimate interests of CUTM and is clearly necessary for the performance of institutional functions (e.g., sharing a staff member's work contact details for a professional enquiry)
  ii. CUTM is legally obliged to make the disclosure (e.g., statutory returns to UGC, NAAC, NIRF, AISHE, government bodies)
  iii. The disclosure is necessary for the performance of a contract to which the Data Principal is a party
  iv. The Data Principal has given prior consent to the disclosure

- Disclosure to law enforcement or regulatory authorities is permitted only where CUTM is under a legal obligation to do so or to prevent serious harm to an individual. All such requests shall be channelled through the DPO or Registrar.
- Staff receiving telephone or email enquiries about whether a named individual is a student or employee of CUTM shall not confirm or deny such membership unless:

  i. Consent has been given by the individual concerned or
  ii. A lawful basis for disclosure exists (e.g., legal obligation, court order)

- As an alternative to disclosure, CUTM may offer to pass a message to the Data Principal asking them to contact the enquirer, without confirming the individual's association with the University.
- Where Personal Data is to be shared with a third party under contract, approved data processing clauses must be included in the contract. The DPO must be consulted before any such contract is signed.

16. Retention and Disposal of Data

- Personal Data shall not be retained for longer than is necessary for the purpose for which it was collected or as required by applicable law or regulation. CUTM shall maintain a Retention and Disposal Schedule specifying retention periods for different categories of data.
- Student Records: Core academic records (admissions data, examination results, degrees awarded) maintained in CUTM's Student Information System shall be retained permanently to support the issuance of transcripts and certificates throughout a student's professional life. Other student records shall be retained in accordance with the Retention and Disposal Schedule.
- Staff Records: Core employment records (name, designation, service history, final pay) shall be retained indefinitely. Other HR records shall be retained for the periods specified in the Retention and Disposal Schedule, which accounts for statutory requirements under the Employees' Provident Funds Act, Income Tax Act and other applicable legislation.
- Recruitment Records: Records pertaining to unsuccessful applicants shall be retained for six months from the date of the final selection decision and then securely destroyed. HR may retain a record of names of applicants, shortlisted candidates and appointees for administrative purposes.
- Disposal: Personal Data being disposed of shall be destroyed in a manner that protects the rights and privacy of Data Principals. Physical records shall be shredded or disposed of as confidential waste. Electronic data shall be securely deleted using appropriate tools. Storage media from decommissioned hardware shall be physically destroyed.
- CUTM shall discourage unnecessary duplication of Personal Data. Where centralised data sources exist (e.g., the Student Information System, HRMS), these shall be used

as the authoritative record. Subsidiary records shall be synchronised with central systems and disposed of when no longer required.

17. Transfer of Personal Data

- Transfer of Personal Data within India shall comply with the provisions of this policy and applicable Data Protection Laws. Personal Data shall be transferred to other organisations only on the basis of a valid data processing agreement or other lawful basis.
- Cross-border transfers: Under the DPDPA 2023, Personal Data may be transferred outside India only to countries or territories notified by the Central Government as permitting such transfers or in accordance with any other conditions prescribed. Staff and researchers must consult the DPO before transferring Personal Data to entities outside India.
- International research collaborations and Memoranda of Understanding (MoUs) with foreign institutions involving the exchange of Personal Data must include appropriate data protection provisions reviewed by the DPO.
- Publishing information on CUTM's public website or platforms accessible internationally constitutes a transfer of data outside India. Staff must ensure that any Personal Data published online has a lawful basis, including appropriate consent where required.

18. Publication of University Information

- CUTM publishes certain categories of Personal Data in the normal course of its academic and administrative functions, including:

  i. Names and profiles of faculty on the CUTM website, including designations, qualifications, research interests and professional photographs
  ii. Names of members of statutory and advisory bodies (Governing Board, Academic Council, Board of Studies, etc.)
  iii. Awards, honours and distinctions conferred by the University
  iv. Staff telephone and email directories (restricted to institutional network where appropriate)
  v. Graduation programmes, convocation videos and ceremony records

vi. Information in prospectuses, annual reports and institutional publications
vii. Press releases, social media posts and public relations materials

- Where any individual requests that their Personal Data in these categories remain confidential or be removed from public platforms, CUTM shall use its best endeavours to comply, subject to any statutory requirement to publish such information.

19. Direct Marketing and Communications

- Any direct marketing communications directed at specific individuals (whether students, prospective students, alumni or other stakeholders) using CUTM systems or data must be approved in advance by the DPO in consultation with the Communications or Admissions office.
- Electronic marketing communications (email, SMS, WhatsApp, social media messages) shall only be sent to individuals who have opted-in to receiving such communications, except where an existing relationship exists in relation to the services being marketed.
- All marketing communications shall include a clear and easy mechanism to opt out. Opt-out requests must be actioned promptly. CUTM shall not make further marketing communications to an individual after receipt of an opt-out request.

20. Use of CCTV and Surveillance Systems

- CUTM operates CCTV and electronic surveillance systems at certain campus locations for the purposes of campus safety, crime prevention and the protection of University assets and the welfare of its community.
- Processing of Personal Data obtained through CCTV is subject to CUTM's CCTV Policy (a separate instrument). The following principles apply:

i. CCTV footage may only be accessed by the Security Manager, senior management and authorised personnel
ii. Footage shall be retained only as long as necessary for the purpose for which it was recorded, in accordance with the Retention and Disposal Schedule
iii. Footage shall not be disclosed to third parties except where required by law, court order or for the prevention or detection of crime

iv. Signage shall be displayed at all CCTV-monitored locations informing individuals that surveillance is in operation

21. Academic Research

- Personal Data collected for academic research purposes must be processed in accordance with this policy, applicable Data Protection Laws and CUTM's Research Ethics and Integrity Policy. Researchers must obtain ethical clearance from the relevant Institutional Ethics Committee (IEC) or Research Ethics Committee (REC) before collecting Personal Data.
- Data collected for research may be processed under the lawful basis of public interest or legitimate interest, provided appropriate safeguards are applied. Where required, the explicit consent of research participants must be obtained.
- Research data shall be anonymised or pseudonymised wherever possible. Identified Personal Data shall be kept only as long as is necessary for the research and then deleted or anonymised.
- Published research outputs must not include information that could identify individual participants without their explicit consent.
- Researchers using data obtained from external sources (government databases, hospital records, industry data) must ensure that appropriate permissions and data sharing agreements are in place before processing commences.

22. Data Protection Impact Assessment (DPIA)

- CUTM shall adopt a Privacy by Design approach, integrating data protection considerations from the outset of any new project, system or process that involves the processing of Personal Data.
- A Data Protection Impact Assessment (DPIA) shall be conducted before commencing any processing activity that is likely to result in a high risk to the rights of Data Principals, including:

  i. Large-scale processing of Sensitive Personal Data
  ii. Systematic monitoring of individuals on campus using surveillance technologies
  iii. Adoption of new information systems involving biometric data (e.g., attendance management)
  iv. Automated processing that produces decisions with significant effects on individuals
  v. Processing involving student performance analytics, tracking or profiling

- A DPIA shall document: the nature and purpose of the processing; the legal basis; a risk assessment identifying potential harms to Data Principals; and the mitigation measures to be applied.
- DPIAs shall be maintained and reviewed periodically. They shall be submitted to the DPO for review and approval before processing commences.
- Staff are encouraged to consult the DPO when initiating any new project involving Personal Data, even where a formal DPIA is not legally required.

23. Training and Awareness

- CUTM shall ensure that all staff receive adequate training on data protection principles, their responsibilities under this policy and the procedures to be followed in the event of a data breach.
- Mandatory induction training on data protection shall be provided to all new staff. Refresher training shall be conducted at intervals not exceeding two years or more frequently where there are significant changes to Data Protection Laws or CUTM's processing activities.

- Specialised training shall be provided to staff with significant responsibilities for processing Personal Data, including system administrators, admissions officers, HR staff and research supervisors.
- Awareness materials, FAQs and data protection guidance shall be made available to all staff and students on CUTM's intranet.

24. Approval and Review

This policy has been approved by the university administration and will be reviewed periodically to ensure its effectiveness and compliance with current laws and best practices.Any amendments to the policy will be communicated to the university community.

Anita Patra

Dr. Anita Patra
Registrar

Centurion University of Technology and Management

REGISTRAR
Centurion University of
Technology & Management
ODISHA

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT, ODISHA

CAMPUSES:

Paralakhemundi Campus
Village Alluri Nagar
P.O. – R Sitapur, Via- Uppalada
Paralakhemundi, Dist.- Gajapati
Odisha, India. PIN– 761211

Bhubaneswar Campus
Ramchandrapur
P.O. – Jatni, Bhubaneswar
Dist.- Khurda, Odisha,
India, PIN– 752050

Balangir Campus
Behind BSNL Office
IDCO land, Rajib Nagar
Dist.- Balangir, Odisha
India, PIN-767001

Rayagada Campus
IDCO Industrial Area
Pitamahal, Rayagada
Dist.-Rayagada, Odisha
India, PIN-765001

Balasore Campus
Gopalpur,
P.O.-Balasore
Dist.-Balasore, Odisha
India, PIN-756044

Chatrapur Campus
Ramchandrapur,
Kaliabali Chhak,
P.O-Chatrapur, Dist.-Ganjam
Odisha, India, PIN-761020