POLICY & STANDARD OPERATING PROCEDURE FOR DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023 INSTITUTIONAL POLICY

Document Number	:	IQAC/120/22
Document Name		Policy & Standard Operating Procedure for Digital Personal Data Protection (Dpdp) Act, 2023 Institutional Policy
Policy Category	:	IQAC Policy
Version Number	:	1.0
Effective Date	:	01 August 2026
Applicable to	:	All internal and external stakeholders of AMGOI
Prepared By	:	Head Department of CSE
Reviewed By	:	Dean, IQAC
Approved By	:	Director & Campus Director, AMGOI

1. Purpose

The purpose of this Policy is to establish an institutional framework for the lawful, fair, transparent, secure and accountable processing of digital personal data by Ashokrao Mane Group of Institutions (AMGOI). The Policy seeks to protect the privacy and rights of individuals whose personal data is processed in connection with admission, teaching-learning, examination, research, employment, administration, campus services, communication and other legitimate institutional functions.

The Institute shall implement this Policy in accordance with the Digital Personal Data Protection Act, 2023 (DPDP Act), applicable rules and notifications in force, and other applicable legal, regulatory and contractual requirements.

2. Objectives

1. Establish a consistent institutional approach for handling digital personal data throughout its lifecycle, from collection to secure deletion or anonymisation.
2. Ensure that personal data is processed for a specified, lawful and clearly communicated purpose and only to the extent reasonably necessary for that purpose.
3. Promote transparent notices and valid consent wherever consent is the applicable basis for processing, including a practical mechanism to withdraw consent.
4. Protect the rights of Data Principals, including applicable rights relating to access to information, correction, completion, updating, erasure, grievance redressal and nomination, subject to the Act and applicable rules.
5. Define accountability and responsibilities of the Director/Campus Director, Dean IQAC, Deans, Heads of Departments, faculty, students, administrative units, IT personnel and authorised service providers.
6. Implement appropriate technical and organisational safeguards to prevent unauthorised access, disclosure, alteration, loss, misuse or destruction of personal data.
7. Establish procedures for data-breach reporting, assessment, response, documentation and notification in accordance with applicable legal requirements.
8. Ensure that third-party service providers and data processors handle personal data only under documented instructions and appropriate contractual safeguards.
9. Create awareness and build capacity among stakeholders through periodic training, communication and monitoring.

10. Maintain records, evidence and review mechanisms to support compliance, accountability, audit and continuous improvement.

3. Scope

This Policy applies to:

- The Institute and its management, Director, Campus Director, Deans, Dean IQAC, Heads of Departments, faculty members, non-teaching staff, students, researchers, temporary personnel, consultants, contractors and authorised visitors, to the extent their activities involve institutional personal data.
- Applicants, students, parents/guardians, alumni, employees, prospective employees, vendors, donors, visitors, industry partners and other individuals whose personal data is processed by or on behalf of the Institute.
- Personal data processed in digital form, including data collected directly or received from authorised sources and data converted into digital form, where the DPDP Act applies.
- Institutional systems and records, including admission and student-information systems, ERP, LMS, examination systems, HR/payroll systems, websites, mobile applications, email, digital attendance, CCTV or access-control systems, online forms, cloud services, research platforms, backups and portable storage devices.
- Processing carried out on campus, remotely or through an authorised third-party service provider, subject to applicable law and the Institute's approved arrangements.

The Policy shall be read subject to the scope, exemptions, commencement provisions and requirements of the DPDP Act and applicable rules. Where another law imposes additional or stricter requirements, the relevant legal/compliance authority shall determine the applicable approach.

4. Definitions

1. Personal Data – Any data about an individual who is identifiable by or in relation to such data, as defined by applicable law.

2. Data Principal – The individual to whom the personal data relates; for a child or a person with a disability, the parent, lawful guardian or other person recognised under the Act may act as applicable.

3. Data Fiduciary – The person who, alone or in conjunction with others, determines the purpose and means of processing personal data. The Institute shall assess its role for each processing activity.

4. Data Processor – A person who processes personal data on behalf of a Data Fiduciary.

5. Processing – A wholly or partly automated operation or set of operations performed on digital personal data, as covered by the Act.

6. Consent – A free, specific, informed, unconditional and unambiguous indication of agreement through a clear affirmative action, where consent is the applicable basis under the Act.

7. Data breach – Any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access that compromises confidentiality, integrity or availability, as relevant under applicable law.

8. Child – An individual below the age specified in the DPDP Act, requirements relating to parental or lawful guardian consent and child-specific safeguards shall be applied as legally required.

9. Personal data inventory – A maintained record of categories of personal data, purposes, data subjects, systems, authorised users, recipients, retention criteria and safeguards.

Terms not defined in this Policy shall have the meanings assigned to them in the DPDP Act and applicable rules.

5. Policy Guidelines

5.1 Lawful, Fair and Transparent Processing: Personal data shall be processed lawfully, fairly and transparently, with clear privacy notices explaining the purpose, data collected, applicable rights and grievance redressal mechanism.

5.2 Purpose Limitation and Data Minimisation: Only necessary personal data shall be collected for specified institutional or legal purposes and shall not be used for incompatible purposes without a lawful basis.

5.3 Consent and Consent Withdrawal: Consent shall be obtained and recorded wherever required, with an accessible withdrawal mechanism and appropriate action in accordance with applicable law.

5.4 Children and Persons Requiring a Lawful Guardian: Personal data of children and persons requiring a lawful guardian shall be processed with the required verification, consent and safeguards under the DPDP Act.

5.5 Accuracy, Access and Data Quality: Personal data shall be maintained accurately, accessed only by authorised personnel, and corrected, updated or erased upon valid requests in accordance with applicable requirements.

5.6 Security Safeguards: Appropriate technical and organisational security measures shall be implemented to protect personal data against unauthorised access, disclosure, loss, alteration or misuse.

5.7 Data Retention, Erasure and Disposal: Personal data shall be retained only for the approved or legally required period and securely erased, anonymised or disposed of when no longer required.

5.8 Sharing, Disclosure and Third-Party Processors: Personal data shall be shared only for authorised purposes, with appropriate approvals, security assessments, contractual safeguards and compliance with applicable transfer requirements.

5.9 Data Principal Rights and Grievance Redressal: The Institute shall establish an accessible mechanism to receive, track and resolve Data Principal requests and grievances within applicable timelines through the designated authority.

5.10 Data Breach and Incident Management: Any suspected or actual personal data breach shall be promptly reported, investigated, contained, documented and notified to affected individuals and authorities as required by applicable law.

5.11 Research, Photographs, Events and Communications: Research activities, surveys, events, photographs, recordings and publications involving personal data shall comply with applicable privacy, notice, consent and security requirements.

5.12 Confidentiality, Training and Accountability: All stakeholders shall maintain confidentiality, participate in periodic data protection awareness programmes and comply with institutional policies, with violations addressed through appropriate disciplinary or contractual measures.

6. Roles and Responsibilities

A. **Director / Campus Director:** Provide institutional leadership, approve the DPDP Policy and resources, designate responsible officers, and oversee compliance, security risks, incidents, audits and data-protection requirements in institutional agreements.

B. **Dean IQAC:** Coordinate policy implementation, develop annual compliance and awareness plans, monitor departmental reports, maintain compliance evidence and facilitate periodic reviews and continuous improvement.

C. **All Deans:** Ensure policy compliance within their respective academic and administrative units, designate data owners, implement appropriate privacy and security practices, and monitor training and reporting.

D. **Heads of Departments (HoDs):** Maintain departmental data inventories, ensure lawful data collection and secure access, coordinate rights requests and incident reporting, enforce retention and disposal procedures, and submit compliance reports.

E. **Faculty Members:** Handle student, staff and research-participant data only for authorised purposes, maintain confidentiality, use approved privacy procedures, safeguard records and devices, and report suspected data breaches promptly.

F. **Students:** Use personal data responsibly for authorised academic activities, protect confidential information and account credentials, follow institutional privacy guidelines, complete required awareness training and report suspected data exposure.

G. **IT Head / System Administrator:** Implement and maintain technical security safeguards, access controls, backups and monitoring, support incident investigation and secure deletion, assess vendor security arrangements, and report significant risks.

H. **Registrar / Designated Grievance or Privacy Officer:** Manage privacy-related requests and grievances, coordinate verification and timely resolution, maintain compliance records, and coordinate breach assessment and statutory notifications in accordance with the formally assigned role and applicable law.

I. **Administrative Units / Procurement / HR / Admissions / Examinations:** Collect and maintain necessary records accurately, use approved systems and privacy notices, restrict access, follow retention schedules, ensure vendor and process compliance, and escalate requests or incidents appropriately.

J. **Third-Party Service Providers / Data Processors:** Process personal data only on authorised instructions, maintain confidentiality and security, promptly report incidents, assist with rights requests and audits, and securely return or delete data in accordance with contractual terms and applicable law.

7. Review and Revision of Policy

The Policy shall be reviewed at least once every three years or earlier in response to legal amendments, government directions, audit findings, security incidents or significant institutional changes. Dean IQAC shall coordinate the review with relevant authorities and departments, document proposed amendments and their implementation requirements, and obtain approval from the Director/Campus Director or competent authority. IQAC shall maintain version history, approval records and controlled copies, archive superseded versions, and facilitate urgent interim instructions when required, followed by formal policy revision.

8. Annexures/Supporting Documents

Annexure A – Personal Data Inventory and Processing Register.

Annexure B – Privacy Notice and Consent Template (including purpose, data categories, lawful basis, recipients, retention, rights and grievance channel).

Annexure C – Consent Withdrawal and Data Principal Request Form / Request Register.

Annexure D – Personal Data Breach / Security Incident Reporting Form and Incident Register.
Annexure E – Data Retention and Secure Disposal Schedule, including deletion approval and evidence.
Annexure F – Third-Party / Data Processor Due-Diligence Checklist and Data Processing Agreement checklist.
Annexure G – Role-Based Access Request, Approval and Periodic Review Form.
Annexure H – Annual DPDP Compliance Checklist and Departmental Self-Assessment Report.
Annexure I – Training Attendance, Awareness Material and Acknowledgement of Confidentiality.
Annexure J – Data Sharing / Disclosure Approval Record.
Annexure K – Data Breach Response Checklist and Post-Incident Review Template.

The annexures listed above are supporting-document requirements and may be issued as controlled templates by IQAC/Administration/IT. The Institute shall ensure that the final versions reflect the applicable statutory forms, timelines and directions in force. Existing institutional policies on IT security, records management, research ethics, student records, HR, CCTV, procurement and grievance redressal shall be read together with this Policy.

9. Standard Operating Procedure (SOP)

1. Annual Implementation Planning: Dean IQAC shall communicate the annual DPDP implementation calendar, compliance requirements, reporting formats and training plan to all concerned units.
2. Designation of Responsible Officers: The Director/Campus Director shall designate responsible officers for privacy, grievance handling and incident coordination and publish their current contact details.
3. Personal Data Inventory: Each Dean, HoD and administrative head shall identify and document the personal data handled by their unit, its purpose, storage, access, sharing and retention details in Annexure A.
4. Lawful Processing and Privacy Notices: Each unit shall verify the lawful basis, notice, consent and child/guardian requirements before processing personal data, referring unclear or high-risk cases to the designated officer.
5. Consent Management: Where required, units shall obtain and record valid consent using approved notices and provide an accessible mechanism for withdrawal.
6. Privacy Risk Assessment: New systems, forms, research activities, events, vendor arrangements or significant processing changes shall undergo appropriate privacy and security assessments in consultation with IT and the designated officer.
7. Access Control: HoDs and administrative heads shall approve access only for authorised users, while IT shall implement, monitor and revise access permissions as required.
8. Data Storage and Sharing: Personal data shall be stored in approved systems and shared only for authorised purposes, with appropriate approvals and contractual safeguards for third-party processing.
9. Data Retention and Disposal: Units shall follow approved retention schedules and ensure secure deletion or anonymisation of data when no longer required and when legally permissible, documenting disposal where appropriate.
10. Data Principal Requests: Requests shall be received, logged, verified, assigned and resolved through the designated channel within applicable timelines, with reasons and escalation details documented where necessary.
11. Incident Reporting: Any suspected or actual personal-data breach shall be reported immediately to IT and the designated officer without waiting for a complete investigation.

12. Incident Investigation and Remediation: IT and the designated officer shall contain incidents, preserve evidence, assess impact, coordinate corrective measures and document findings in consultation with institutional leadership and legal support where necessary.

13. Statutory Notifications: The authorised institutional officer shall coordinate and document notifications to affected individuals and relevant authorities within the timelines prescribed by applicable law.

14. Semester-wise Compliance Reporting: Each Dean, HoD and administrative head shall submit a semester-wise compliance report to Dean IQAC covering data inventories, consent, requests, incidents, access controls, disposal, vendors, training and pending corrective actions.

15. Monitoring and Escalation: Dean IQAC shall review consolidated reports, coordinate corrective actions with deadlines and escalate significant risks, serious incidents and overdue actions to the Director/Campus Director.

16. Annual Institutional Review: Dean IQAC shall prepare an annual DPDP implementation report covering compliance status, training, incidents, audits, corrective actions and priorities for the next academic year.

17. Document Control and Communication: IQAC shall communicate approved policy updates and procedures, maintain controlled document versions and preserve relevant compliance evidence for audits and institutional review.

10. Monitoring, Reporting and Non Compliance

- Compliance shall be monitored through departmental self-assessments, access reviews, sample checks, training records, incident/request registers, vendor reviews and internal audits, as appropriate.
- Each unit shall nominate a data owner or coordinator for its records and respond to IQAC/IT/designated officer requests for evidence within the communicated timeline.
- Non-compliance shall be documented with risk level, corrective action, responsible person and target completion date. Unresolved or high-risk matters shall be escalated to the Director/Campus Director.
- Violations may lead to remedial instruction, access restriction, disciplinary action under applicable institutional rules, contractual remedies and/or statutory consequences, subject to due process.

11. Implementation Checklist

- Approved DPDP Policy, designated officer details, personal data inventory and data owners established.
- Privacy notices, consent records, access controls, secure storage, transfer, backup and deletion procedures maintained.
- Grievance handling, incident reporting, third-party agreements and privacy awareness training implemented and documented.
- Periodic departmental compliance reports, audit findings and corrective actions submitted to IQAC.

Prof. A. B. Rabade
Dean, IQAC

Dr. Mrs. S. R. Chougule
Director
Shri Balasaheb Mane Shikshan Prasarak Mandal's
Ashokrao Mane Group Of Institutions
Vathar Tarf Vadgaon, Tal. Hatkanangale
Dist. Kolhapur, Maharashtra - 416112

Dr. P. B. Ghewari
Campus Director
CAMPUS DIRECTOR
SHRI BALASAHEB MANE SHIKSHAN PRASARAK MANDAL'S
ASHOKRAO MANE GROUP OF INSTITUTIONS
Vathar Tarf Vadgaon, Tal. Hatkanangale, Dist. Kolhapur, M.S. 416112