ManageEngine
Endpoint Central

Data Protection Policy for Educational Institutions

Introduction

The purpose of this policy is to ensure the security and confidentiality of personal and sensitive data within the educational institution. This policy outlines the institution's commitment to data protection and the measures taken to safeguard personal data against unauthorized access, disclosure, alteration, and destruction.

Scope

This policy applies to all employees, students, contractors, and third-party service providers who handle or have access to personal data managed by the institution.

Definitions

- **Personal data :** Any information relating to an identified or identifiable person.
- **Data processing :** Any operation performed on personal data, such as collection, storage, use, or disclosure.
- **Data subject :** Any individual whose personal data is being processed.

Data classification

Data is classified into the following categories to determine the level of protection required

- **Public data :** Information intended for public use.
- **Internal data :** Information restricted to internal use within the institution that may not necessarily be sensitive information.
- **Confidential data :** Sensitive information requiring higher levels of protection.
- **Restricted data:** Highly sensitive information with the strictest access controls.

Principles of data protection

- **Lawfulness, fairness, and transparency :** Personal data shall be processed lawfully, fairly, and transparently.
- **Purpose limitation :** Data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data minimization :** Data collection shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

- **Accuracy :** Personal data shall be accurate and, where necessary, kept up to date.
- **Storage limitation :** Data shall be kept in a form that permits identification of data subjects for no longer than necessary.
- **Integrity and confidentiality :** Data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- **Accountability :** The institution shall be responsible for and be able to demonstrate compliance with these principles.

Data subject rights

- **Right to access :** Individuals can request access to their personal data.
- **Right to rectification :** Individuals can request correction of inaccurate or incomplete data.
- **Right to erasure :** Individuals can request deletion of their personal data under certain conditions.
- **Right to restriction of processing :** Individuals can request the restriction of processing under certain circumstances.
- **Right to data portability :** Individuals can request to receive their data in a structured, commonly used format.
- **Right to object :** Individuals can object to processing based on legitimate interests or direct marketing.

Data Protection Officer (DPO)

The institution shall appoint a DPO responsible for

- Monitoring compliance and adherence to this policy and relevant data protection laws.
- Advising on Data Protection Impact Assessments (DPIAs).
- Liaising with regulatory authorities as a point of contact for data protection authorities.
- Promoting awareness of data protection obligations within the institution.

Data collection and use

- Data shall be collected only for legitimate educational purposes.
- Individuals shall be informed about the purpose of data collection, and their consent shall be obtained where necessary.

Data security measures

The institution shall implement appropriate technical and organizational measures to ensure data security, including:

- **Access control :** Restricting access to personal data to authorized personnel only.
- **Encryption :** Encrypting personal data during transmission and storage.
- **Regular audits :** Conducting regular security audits and assessments.
- **Incident response :** Establishing a protocol for responding to data breaches.
- **Training :** Providing regular training on data protection and security practices to staff and students.

Data storage and encryption

- Data shall be stored securely using encryption and other security measures.
- Sensitive data stored on portable devices and media must be encrypted.
- Regular backups shall be performed, and backup data shall be stored securely
- Data transmitted over networks shall be protected using encryption (e.g., SSL/TLS).
- Secure methods of file transfer (e.g., SFTP) shall be used for transmitting sensitive data.

Data retention and disposal

- Data retention periods shall be defined based on legal, regulatory, and institutional requirements.
- Data shall be securely deleted or destroyed when it is no longer needed.

Data breach management

- A data breach response plan shall be established to address data breaches and security incidents.
- All staff, faculty, and students must report suspected data breaches immediately.
- In the event of a breach, the incident must be reported to the Data Protection Officer (DPO) immediately.
- Steps shall be taken to contain the breach and recover any compromised data.
- If the breach is likely to result in a high risk to the rights and freedoms of individuals, affected data subjects and relevant authorities shall be notified within 72 hours.
- Incidents shall be documented, investigated, and appropriate corrective actions shall be taken.

Training and awareness

- Regular training on data protection policies and best practices shall be provided to staff, faculty, and students.
- Awareness programs shall be conducted to ensure understanding of data protection responsibilities.

Third-party data processing

The institution shall implement appropriate technical and organizational measures to ensure data security, including:

- The institution shall conduct due diligence to ensure they have adequate data protection measures.
- Establish agreements that outline data protection obligations.
- Regularly reviewing and auditing third-party compliance.

Responsibilities

- **Data Protection Officer (DPO) :** Responsible for overseeing the implementation and enforcement of this policy.
- **IT department :** Ensures technical safeguards are in place to protect data.
- **All employees and students :** Responsible for adhering to data protection policies and reporting breaches.

Review and updates

- This policy shall be reviewed and updated annually or as required to reflect changes in legislation, technology, or institutional practices.
- Compliance with this policy shall be monitored, and violations shall be addressed promptly.