DATA PROTECTION POLICY

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS

GDPR	General Data Protection Regulation

DEFINITION OF DATA PROTECTION

All employees, students and other affiliates of {company} have a responsibility to protect the confidentiality, integrity, and availability of {company} information collected, processed, stored or transmitted irrespective of the location or medium on which the information resides.

Protection levels must be established and implemented relative to the information's classification, ensuring against unauthorized access, modification, disclosure and destruction. For information governed by law and regulations (such as student records, personally identifiable information and protected health information), the protection levels must satisfy the respective, data security and data privacy requirements e.g. GDPR

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections. This is not only to ensure compliance with the GDPR but also to provide proof of compliance.

BY THIS POLICY

This data protection policy ensures {company}:

- Complies with data protection laws and follows good practices
- Protects the rights of employees, students, customers and partners
- Is open about how it stores and processes individual's data
- Protects itself form the risks of a data breach

The following policy details the basic requirements and responsibilities for the proper management of information assets at {company}. The policy specifies the means of information handling and transfer within the Business.

APPLIES TO

This data protection policy applies to all the systems, people and business processes that make up the {company}'s information systems. This includes all students, partners, employees and third parties who have access to Information Systems or information used for {company} purposes.

This policy applies to all data that {company} holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone number
- Any other information relating to individuals

POLICY GUIDELINES

General staff guidelines

Employees and students should keep all data secure, by taking sensible precautions and following the guidelines below.

- Strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people. either within the company or externally.
- Personal data
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of according to Data retention policy (coming someday).

Data storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it. These guidelines also apply to data that is stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper, and printouts are not left where unauthorised people could see them, see clean desk policy (coming someday) for more information.
- Sensitive data printouts should be disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- If data is stored on removable media, these should be kept locked away securely.
- Data should only be stored on designated drivers and servers.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently. Those backups should be tested regularly.

Roles and Responsibilities

All students, employees and third parties of {company} has responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data must ensure that it is handled and processed in line with this policy. However, these people have key areas of responsibility: {list people}

POLICY COMPLIANCE

Exceptions

Non-compliance with this policy by any member of {company} may result in disciplinary action.

Non-Compliance

Non-compliance with this policy by any member of {company} may result in disciplinary action.

RELATED STANDARDS, POLICIES AND PROCESSES

None

REVISION HISTORY

Version	Description	Date	Author	Approved By
1.0	Initial version	14/04/2025	ztothez	