AIMS COLLEGE OF BUSINESS AND IT (PVT) LTD

DATA PROTECTION POLICY

AIMS CAMPUS
TRANSFORMING LIVES

Data Protection Policy

This policy applies to personal data, which is any data that may be used to identify an individual, either directly or in conjunction with other data that you may have or come into possession of. Certain sorts of personal data are very sensitive.

This is known as special category data, and it must be handled with extreme caution. Data regarding race, ethnicity, religion, medical/health data, and political affiliations, genetic or biometric information are examples of special category data.

Our Sensitive Data Policy has more information on how and why we treat special category data. Compliance with this policy is a prerequisite for employment or study at AIMS. Noncompliance with the policy's responsibilities may result in disciplinary action. Data protection legislation imposes requirements. If you use a non-AIMS controlled device to handle personal data (for example, through an instant messaging service), you are required to follow the data protection rules.

In the case of a data breach or suspected breach, employees and students must contact the Data Protection Officer as soon as possible at arc@aimscollege.edu.lk.

On its dedicated intranet sites, a member from our Audit and Risk Committee will provide a variety of tools and assistance to assist Schools and Services in complying with information legislation.

Scope

This policy applies to anybody or any organization that processes personal data for or on behalf of another business associated with our operations.

Personal data processing happens when an action is performed on the personal data to accomplish a function. Identification, collecting, recording, organizing, structuring, storing, modification, retrieval, consultation, usage, disclosure by any means, limitation, erasure, or destruction of personal data are all examples of processing activities.

This policy applies to any electronic processing of personal data, including electronic mail, documents prepared using word processing software, programs, software, and manual files structured in a way that gives easy access to information about persons.

Data Collection and Processing Goals

To sustain its essential activities, AIMS must collect and keep a wide range of personal and special category data on its workers, students, and other users of AIMS facilities. To be in compliance with the law, AIMS and anybody else in charge of processing personal data on its behalf must:

- Implement the appropriate controls, technical and organizational measures required to demonstrate compliance with the data protection principles
- Allow a person to exercise their Information Rights and adhere to approved data protection codes of conduct
- Only use personal data for clear and specified purposes
- Only keep personal data for as long as is reasonably required

Data Protection Guidelines

Personal data collection, use, retention, transfer, disclosure, and destruction are governed by the following principles. When processing personal data, these principles must be observed. Further advice and information on how to apply these principles may be obtained on the Intranet site of the Audit and Risk Committee.

- Lawfulness, Fairness, and Transparency - Personal data shall be processed lawfully, fairly, and transparently.
- Purpose Limitation - Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be used for other purposes where such use would be incompatible with the initial purpose.
- Data Minimization - Personal data shall be adequate, relevant, and limited to what is necessary for the purpose for which it was collected.

- Accuracy - Personal Data must be correct and, when required, kept up to date.
- Storage Restrictions - Personal data should be stored in a manner that allows Data Subjects to be identified for no longer than is required.
- Integrity and Confidentiality - Personal data must be processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage to that data.
- Accountability - demonstrating how we comply with the law by having documented processes, procedures, and policies in place.

Responsibilities

At the Senior Management level, the Executive Board has delegated responsibility for personal data security to a designated Audit and Risk Committee Chair (ARC). The ARC Chair has the authority to act independently and is ultimately responsible for ensuring that AIMS data protection requirements are met. The ARC's function is independent in order to comply with the duties set forth in the General Data Protection Regulation, and they report to the highest level of management within the organization. In addition, the ARC Chair serves as the initial point of contact for Supervisory Authorities and persons whose data is handled.

Each Head of Department is responsible for promoting and modeling best data protection practices within their teams, as well as keeping the ARC Chair informed of changes in the collection, usage, and security measures used for personal data processing within the School, Service, or Unit. To achieve this obligation, the Information Assurance Office will train AIMS personnel to serve as Data Protection Advisors, advocating best practices and reporting concerns within their respective departments. Senior management, employees, and students all have data protection duties.

Rights to Information

Every individual about whom AIMS processes personal data has rights on how the data is used and handled. When an individual submits a request relating to any of their information rights, AIMS will review each request in compliance with all applicable laws and regulations. Every user that processes personal data for AIMS purposes must work with the Information Assurance Office to meet our duties related to responding to information rights requests.

Working from a Distance/Home

The principles and requirements of the Personal Data Protection Act, No. 9 of 2022 continue to apply when working remotely. All employees are obliged to keep any data they process from home safe and distinct from other files or documents (even on their own personal devices or on paper).

Data in specific programs, like Office 365, will be safeguarded by multi-factor authentication and other safeguards, such as data encryption and the potential restriction of downloading and sharing capabilities.

When using personal equipment such as laptops, employees are obliged to keep software up to date and anti-virus software installed. Staff must utilize their AIMS email, Microsoft Teams, OneDrive, or SharePoint accounts to communicate data. It is not permissible to share AIMS data via personal email accounts, personal cloud storage, or communication platforms.

Software and hardware recommendations

IT Services offer and support a range of systems, applications and services to meet the core business purposes of AIMS. These supported systems have been assessed to ensure that they meet our requirements regarding functionality, storage of data, disaster recovery, security and regulatory compliance with data protection and other relevant laws. Any staff or students that wish to use applications, software or services that are not recommended by IT Services are responsible for ensuring that appropriate controls are in place to allow AIMS to comply with the obligations of the Data Protection Act and other relevant laws. Due to the complex nature of

compliance, it is strongly recommended that you check with IT Services before using new systems, apps or services.

Where applicable, the Information Assurance Office will assist in assessing compliance; however, before personal data is handled, you must notify the Information Assurance Office or a delegated representative that an evaluation of an unsupported application, system, or service is necessary.

When the usage of an unsupported system, application, or service is assessed to constitute a danger to the institution, ARC Chair or designated representative will outline these risks, as well as potential mitigation measures. If you choose not to apply the recommended mitigations and accept the degree of risk, the Information Assurance Office will request approval of these risks through the use of a Risk approval Form signed by the relevant Head or Director of Service, which will be maintained under frequent review.

In cases where such systems, applications, or services have the potential to breach our data protection obligations (e.g., by failing to comply with data protection principles), the ARC Chair has a legal obligation to notify the relevant Heads or Directors, and if necessary, the Executive Board. Such violations impose a legal requirement on AIMS to cease processing personal data in a manner that violates the law, and in such circumstances, the Information Assurance Office will take urgent action to ensure the institution remains in compliance with its duties.

Requests and Disclosures from Law Enforcement

Personal data may be disclosed without the knowledge or agreement of a Data Subject in certain circumstances. This is the situation when personal data must be disclosed for any of the following reasons: Crime prevention or detection.

Offenders are apprehended or prosecuted. The collection or assessment of a tax or charge. By a court's order or any rule of law.

If AIMS or a recognized third-party processes personal data for one of these objectives, it may deviate from the processing restrictions specified in this policy, but only to the extent that doing

so would be detrimental. If any employee of AIMS receives a request for information pertaining to personal data stored by AIMS from a court or other regulatory or law enforcement authority, the request must be forwarded to the Data Protection Officer, who will give complete guidance and support.

Data Security Training

All AIMS employees, contractors, temporary workers, and volunteers who have access to personal data shall be informed of their duties under this policy as part of their staff induction training, which will include data protection training. Bespoke data protection training is provided for regions that process large amounts of personal data or special category data.

All AIMS employees and students have access to a dedicated data protection intranet site that describes important duties and provides tools to ensure compliance.

Transfers and sharing of data

AIMS may disclose or transfer personal data or special category data to internal recipients or other organizations (Data Processors) in order for them to deliver services on our behalf. AIMS and its businesses will only transmit or exchange personal data with third parties, or enable access to them, if they are certain that the information will be treated legally and responsibly by the receiver and/or data processor.

Handling of Complaints

Data Subjects who wish to lodge a complaint concerning the processing of their personal data should do so in the first place in writing to the Audit and Risk Committe. Complaints will be reviewed on an individual basis, and if appropriate, an inquiry will be performed. Within a

reasonable time, the ARC Chair or a designated representative will inform the Data Subject of the status and resolution of the complaint.

Breach Notification

Anyone who thinks a personal data breach has occurred as a result of the theft, loss, or exposure of personal data must promptly contact the ARC Committee and provide a detailed account of what happened. The event may be reported by e-mail at arc@aimscampus.edu.lk .

All reported occurrences will be investigated by the ARC or an authorized representative to determine if a personal data breach has occurred. If verified, the ARC will pursue the appropriate authorized process based on the importance and volume of the personal data concerned. In the event of a catastrophic personal data breach, the ARC will convene and lead an emergency response team to coordinate and manage the personal data breach response, including informing the appropriate Supervisory Authority if necessary.

Data Retention

Some types of information will be kept for a longer period of time than others due to legal, financial, archival, or other business obligations. AIMS will dispose of any personal data that no longer serves a function in accordance with the storage restriction principle. To apply standard retention durations to our most regularly gathered data, we created a Records Retention Schedule that outlines current retention terms.

CCTV

AIMS runs CCTV systems on all campuses, including static cameras.

The CCTV installations serve the following purposes:

• Protection of AIMS employees, students, visitors, and assets

• The prevention, investigation, and detection of crime and disciplinary offenses in accordance with AIMS disciplinary procedures

• The arrest and prosecution of offenders (including the use of images/data as evidence in criminal / civil proceedings)

• The monitoring of premises security

Network and account monitoring

AIMS employs a variety of preventative measures to safeguard personal information, technology, infrastructure, computer networks, and intellectual property. Every user on our network receives a unique username and password for their own user account. IT Services can audit any activities made on this account because they are logged. This includes, but is not limited to:

• any websites viewed while signed into your AIMS account

• any email sent or received by your AIMS email address

• any Microsoft Teams instant messages sent or received

To limit the danger of large amounts of personal data leaving our network via any Office 365 conduit, including email, OneDrive for Business, or SharePoint, AIMS employs Data Loss Prevention technology. When we get a report of such behavior, our Audit and Risk Committee will investigate to ensure that the sharing of personal data is in accordance with information legislation.

Offenses against Data Protection

It is an offense under the Data Protection Act to:

- obtain, disclose, sell, or propose to sell personal data from AIMS systems without AIMS's authorization
- Retain personal data outside the scope of your work or after your employment ends without the approval of AIMS

- Alter, erase, or conceal personal data to avoid a legitimate disclosure
- Recklessly re-identify de-identified personal data without the consent of AIMS

If there is proof of a violation of the The Personal Data Protection Act, No. 9 of 2022, the situation will be investigated using our disciplinary processes.

If an offense is proven to have been committed, consequences may include dismissal or expulsion.