

UBI Business School Data Protection and Prevention

Policy Owner: Legal Department
Version: D1.0.2
Last Review Date: 07 June 2024
Next Review Date: By 06 December 2025

This data protection policy considers obligations under the Data Protection Legislation, which includes the Data Protection Act 2018 (implemented by the General Data Protection Regulations [GDPR])

1. Policy Statement

UBI Business School is committed to protecting the privacy and rights of individuals with regard to their personal data. This Data Protection and Retention Policy outlines the measures taken to ensure the secure handling, storage, and retention of personal data in compliance with the General Data Protection Regulation (GDPR) and other relevant legislation.

2. Scope

This policy applies to all staff, students, contractors, and visitors who have access to or handle personal data on behalf of UBI Business School. It covers all forms of personal data, including digital, physical, and cloud-based data.

3. Responsibilities

- *Data Protection Officer (DPO)*: Responsible for overseeing the implementation of the Data Protection and Retention Policy, providing guidance and support, and ensuring compliance with relevant data protection legislation.
- *Staff and Students*: Responsible for adhering to this policy, following data protection guidelines, and reporting any data protection incidents or concerns.

4. Data Protection Principles

UBI Business School adheres to the following data protection principles:

- *Lawfulness, Fairness, and Transparency*: Personal data must be processed lawfully, fairly, and in a transparent manner.
- *Purpose Limitation*: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- *Data Minimization*: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- *Accuracy*: Personal data must be accurate and, where necessary, kept up to date.
- *Storage Limitation*: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

- *Integrity and Confidentiality:* Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

5. Data Retention

UBI Business School will retain personal data only for as long as is necessary to fulfill the purposes for which it was collected. The university will:

- Establish and maintain a data retention schedule that specifies retention periods for different categories of personal data.
- Regularly review and update the data retention schedule to ensure compliance with relevant legislation and best practices.
- Securely dispose of personal data that is no longer required, in accordance with the data retention schedule and data protection principles.

6. Data Security

UBI Business School will implement appropriate technical and organizational measures to ensure the security of personal data, including:

- Access controls to ensure that only authorized individuals have access to personal data.
- Encryption to protect personal data in transit and at rest.
- Regular security assessments and audits to identify and address vulnerabilities.
- Secure storage and disposal of physical and digital records containing personal data.

7. Data Subject Rights

UBI Business School is committed to upholding the rights of data subjects as outlined in the GDPR. Data subjects have the right to:

- Access their personal data and obtain information about how it is processed.
- Request the rectification of inaccurate or incomplete personal data.
- Request the erasure of their personal data in certain circumstances.
- Request the restriction of processing of their personal data in certain circumstances.
- Object to the processing of their personal data in certain circumstances.
- Data portability, allowing them to receive their personal data in a structured, commonly used, and machine-readable format and transmit it to another controller.

8. Incident Response

- *Reporting:* All staff, students, contractors, and visitors must report any data protection incidents or concerns to the DPO immediately.
- *Investigation:* The DPO will investigate data protection incidents, assess their impact, and take appropriate action to mitigate risks.
- *Communication:* The university will communicate data protection incidents to relevant stakeholders and, if necessary, report incidents to regulatory authorities.

9. Monitoring and Review

This policy will be reviewed by the policy review deadline with the DPO and the School's senior leadership team to ensure its effectiveness and compliance with relevant legislation and best practices. Any updates or changes will be communicated to all members of the School community.