Data Protection Policy

Policy/Procedure Number:	HR002
Date of Approval:	18th May 2026
Effective Date:	1st June 2026
Review Date:	1st June 2027
Person Responsible:	IT/Data Manager
Approved By:	Governing Board
For Information To:	All staff, students and stakeholders

INDEX

1. Principles:

To operate effectively and fulfil its legal obligations, ISBM University [India] London collects, maintains and uses certain personal information about current, past and prospective employees, students, stakeholders, suppliers and other individuals with whom it has dealings.

All such personal information, whether held on computer, paper, or other media, will be obtained, processed, transported, and stored lawfully and securely, in line with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018 (DPA)**.

The University is committed to the following data protection principles. Personal information must:

- Be processed lawfully, fairly and transparently.
- Be collected for specified, explicit and legitimate purposes, and not processed in ways incompatible with those purposes.
- Be adequate, relevant and limited to what is necessary.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary and disposed of securely.
- Be processed in accordance with the data subject's rights.
- Be kept secure against unauthorised or unlawful processing, accidental loss, destruction or damage.
- Not be transferred outside the UK unless appropriate safeguards are in place in line with UK GDPR.

2. Compliance:

To comply with the data protection principles, the University will:

- Observe fully all conditions for fair and lawful collection and use of personal information.
- Identify and document the **lawful bases for processing** personal data under **Article 6 UK GDPR** (e.g., contract, legal obligation, legitimate interests, consent).
- Identify and document the legal conditions for processing **special category data** under **Article 9 UK GDPR** (e.g., employment law obligations, equality monitoring, safeguarding).
- Ensure data is collected only to the extent needed to fulfil operational needs or legal obligations.
- Maintain accurate and up-to-date personal data.
- Retain personal data only in accordance with the University's **Data Retention and Disposal Schedule**.
- Enable individuals to exercise all their UK GDPR rights, including the rights:
  - to be informed,
  - of access,
  - to rectification,
  - to erasure,
  - to restrict processing,
  - to data portability,
  - to object, and
  - in relation to automated decision-making and profiling.

- Take appropriate technical and organisational security measures.
- Ensure transfers of personal data outside the UK are only permitted where safeguards (e.g. adequacy decision, UK standard contractual clauses) are in place.

3. Responsibilities:

- Overall responsibility for ensuring compliance rests with the **Governing Body** and senior leadership (e.g. Accountable Officer).
- Day-to-day oversight rests with the **IT/Data Manager**, supported by the University's appointed **Data Protection Officer (DPO)** (where required).
- All staff are responsible for ensuring that personal information provided to the University is accurate and up to date, and that they follow this policy when handling personal data.
- Any member of staff or student who processes personal data must do so in line with this policy and related procedures.

4. Information about Employees:

The University holds the following personal information about employees for payroll, HR, and administrative purposes:

- Name, address, contact details, next of kin, partner name, NI number, employment history, salary, qualifications, references.

The University may also hold **special category data**, including:

- Racial or ethnic origin, physical or mental health conditions, DBS checks, immigration/visa documents, passport/ID.

Processing of such data will be carried out only where strictly necessary and in line with Article 9 UK GDPR conditions (e.g. employment, equality, health and safety, right-to-work compliance).

5. Access to Information:

- Individuals have the right to request access to their personal data via a **Subject Access Request (SAR)**.
- Requests should be submitted in writing to the **Accountable Officer or Data Protection Officer**.
- The University will normally respond **within one calendar month** of receiving a valid request (extendable by up to two months for complex cases).
- Requests will be processed **free of charge**, unless they are manifestly unfounded or excessive, in which case a reasonable fee may be charged.
- If data is inaccurate, it will be corrected promptly.

6. IT Communications and Monitoring:

The University provides employees and students with access to IT facilities for academic and administrative purposes. Use of these systems is governed by the **IT Communications Policy**. Monitoring may be carried out where lawful and proportionate, in line with data protection and information security obligations.

7. Breach of the Policy

- Any breach of this policy will be regarded as a disciplinary offence under the University's **Disciplinary Procedures**.
- All staff and students are required to report any **data breaches or suspected breaches** immediately to the IT/Data Manager or DPO.
- The University will assess all breaches. Where a breach is likely to result in a risk to individuals' rights and freedoms, it will be reported to the **Information Commissioner's Office (ICO) within 72 hours**.
- If the breach poses a high risk to individuals, they will also be notified without undue delay.
- Concerns about mishandling of personal data may be raised through the University's **Grievance Procedure**