# Data Protection Policy

| | |
|---|---|
| Policy/Procedure Number: | HR002 |
| Date of Approval: | 23rd March 2025 |
| Effective Date: | 1st April 2025 |
| Review Date: | 1st April 2026 |
| 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 needs to collect, maintain and use 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, handled, processed, transported and stored lawfully and correctly, in accordance with the safeguards contained in the Data Protection Act 2018 (DPA) and UK GDPR.

The University is committed to the principles of data protection. These principles require that personal information must:

- Be fairly and lawfully processed and not processed unless specific conditions are met.
- Be obtained for one or more specified, lawful purposes and not processed in any manner incompatible with those purposes.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary.
- Be processed in accordance with the data subject's rights.
- Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage.
- Not be transferred to countries outside the European Economic Area (EEA), unless the country or territory ensures adequate protection for the rights and freedoms of the data subjects.

## 2. Compliance:

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

- Observe fully, all conditions regarding the fair collection and use of personal information.
- Meet its legal obligations to specify the purpose for which information is used.
- Collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with legal obligations.
- Ensure the quality of the personal information used.
- Apply strict checks to determine the length of time personal information is held.
- Ensure that individuals about whom information is held, are able to exercise their rights under the DPA and UK GDPR, including the right to be informed that processing is taking place, the right of access to their own personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase incorrect information.
- Take appropriate technical and University security measures to safeguard personal information.
- Ensure that personal information is not transferred outside the EEA without suitable safeguards.

## 3. Responsibilities:

- Overall responsibility for ensuring that ISBM University complies with its data protection obligations rests with the Governing Body and its assigned senior personnel e.g. the Vice-Chancellor.
- It is the responsibility of all employees to ensure that personal information provided to the University, for example current address, is accurate and up to date. To this end, employees are required to inform the University immediately when changes occur.
- Employees who are involved in the collection, maintenance and processing of personal information about other employees, students, customers, suppliers or any other individuals with whom the University has dealings, are responsible for following the University's rules on good Data Protection practice as notified from time to time by the Executive Board.

## 4. Information about Employees:

The University holds the following personal information about its employees:

- Name
- Address
- Salary
- Partner Name
- Next of Kin
- Telephone Contact Number including emergency contact
- National Insurance Number
- Previous Employment details
- Qualifications
- References

This information is used for Payroll and Administrative purposes.
We also hold the following sensitive personal information about employees:

- Racial or Ethnic origins
- Physical or mental health condition
- DBS check
- Passport copies and/or other ID
- Immigration/visa copies

This information is used for the purpose of Equal Opportunities monitoring / Health and Safety monitoring and confirmation of right to work in the UK

## 5. Access to Information:

Anyone who is the subject of personal information held by the University has the right to make a subject access request. Employees who wish to exercise this right should write to the Vice-Chancellor. The University reserves the right to charge £25 administration fee for responding to such requests. If, as the result of a subject access request, any personal information is found to be incorrect, it will be amended. The University will deal promptly with subject access requests (SAR) and will normally respond within one calendar month starting from the day the SAR is received. If the University needs something from the person making the SAR request to be able to deal with request e.g. ID documents, the time limit will begin once we have received this. If the SAR request is complex or there are more than one SAR in the same request, the response time may be a maximum of three calendar months, starting from the day of receipt. If there is a delay, the person making the request will be informed accordingly.

## 6. IT Communications and Monitoring:

The University provides employees with access to various computer facilities for work and communication purposes. To ensure compliance with all applicable laws in relation to data protection, information security and compliance monitoring, the University has adopted an IT Communications Policy, which should be read in conjunction with this Data Protection Policy.

## 7. Breach of the Policy

Breach of this policy will be regarded as a disciplinary offence and will be dealt with under the University's formal Disciplinary Procedure.

Employees who consider that there has been a breach of this policy in relation to personal information about them held by the University, should raise the matter via the University's formal Grievance Procedure.