Data Protection and UK GDPR Policy (2025)

1. Introduction

IBS Training and Development Ltd ("IBS", "the Centre", "we", "our", or "us") is committed to protecting the privacy and personal data of its students, staff, contractors, partners, and other stakeholders. This Data Protection and UK GDPR Policy sets out how IBS complies with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, ensuring that personal data is processed lawfully, fairly, transparently, and securely.

This policy applies to all personal data processed by IBS during its academic, administrative, operational, and training activities, whether processed electronically, on paper, or by other means.

2. Scope of the Policy

This policy applies to:

- Current, former, and prospective students
- Academic staff, tutors, assessors, and visiting lecturers
- Administrative and support staff
- Contractors, consultants, and third-party service providers
- Applicants, alumni, and external partners

All individuals who process personal data on behalf of IBS must comply with this policy and relevant data protection legislation.

3. Legal Framework

This policy is based on compliance with the following legislation and regulatory guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000 (where applicable)
- Relevant guidance issued by the Information Commissioner's Office (ICO)

4. Data Protection Principles

IBS processes personal data in accordance with the seven data protection principles set out in Article 5 of the UK GDPR:

1. **Lawfulness, fairness and transparency**
2. **Purpose limitation** – data is collected for specified, explicit, and legitimate purposes
3. **Data minimisation** – data is adequate, relevant, and limited to what is necessary

4. **Accuracy** – data is accurate and kept up to date
5. **Storage limitation** – data is retained only for as long as necessary
6. **Integrity and confidentiality** – data is processed securely
7. **Accountability** – IBS takes responsibility for compliance and can demonstrate it

5. Types of Personal Data Processed

IBS may process the following categories of personal data:

5.1 Personal Data

- Name, address, email, telephone number
- Date of birth, nationality
- Student identification numbers
- Academic records, assessments, attendance
- Financial information (fees, funding status)

5.2 Special Category (Sensitive) Data

Where strictly necessary and with appropriate safeguards, IBS may process:

- Health or disability information (for support and reasonable adjustments)
- Equality and diversity monitoring data
- Criminal conviction data (where required by law or awarding bodies)

6. Lawful Bases for Processing

IBS processes personal data only where a lawful basis exists, including:

- **Consent** – where freely given, specific, informed, and unambiguous
- **Contractual necessity** – to fulfil student enrolment and training agreements
- **Legal obligation** – compliance with regulatory, awarding body, or statutory duties
- **Public task** – where applicable to education and training functions
- **Legitimate interests** – provided these do not override individual rights

Special category data is processed under additional lawful conditions set out in Article 9 of the UK GDPR.

7. Consent

Where consent is relied upon, IBS ensures that:

- Consent is clearly documented
- Individuals understand what they are consenting to
- Consent can be withdrawn at any time without detriment

Consent forms, including the **Data Protection and IT Regulations Declaration**, form part of IBS's compliance framework.

8. Data Subject Rights

Individuals whose data is processed by IBS have the following rights:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision-making and profiling

Requests must be made in writing and will be responded to within **one month**, in line with UK GDPR requirements.

9. Data Security

IBS implements appropriate **technical and organisational measures** to protect personal data, including:

- Secure IT systems and password controls
- Role-based access to data
- Encryption and secure storage
- Staff training and awareness
- Secure disposal of data and records

Any breach or suspected breach must be reported immediately to the **Senior Tutor and Head of IT and Information Compliance**.

10. Data Breaches

In the event of a personal data breach, IBS will:

- Investigate the incident promptly
- Contain and mitigate any risks
- Notify the Information Commissioner's Office (ICO) within 72 hours where required
- Inform affected individuals where there is a high risk to their rights and freedoms

All staff and students are required to report suspected breaches without delay.

11. Data Sharing and Disclosure

IBS may share personal data with:

- Awarding and accrediting bodies
- Regulatory authorities
- Government agencies where legally required
- Approved third-party service providers

All data sharing is governed by data sharing agreements and carried out in compliance with UK GDPR.

12. International Data Transfers

Where personal data is transferred outside the UK, IBS ensures that:

- Adequate safeguards are in place
- Transfers comply with UK GDPR requirements
- Approved mechanisms (e.g., adequacy decisions or standard contractual clauses) are used

13. Data Retention

IBS retains personal data only for as long as necessary for the purposes for which it was collected, in accordance with its **Data Retention Schedule**. Data is securely destroyed once retention periods expire.

14. Responsibilities

14.1 IBS Responsibilities

- Maintain and update data protection policies
- Provide training and guidance
- Monitor compliance

- Handle data protection complaints and requests

14.2 Student and Staff Responsibilities

- Process personal data responsibly and lawfully
- Maintain confidentiality
- Report misconduct or data breaches
- Comply with IT and information security policies

15. Complaints

Individuals who believe their data has been mishandled may raise a complaint with IBS in the first instance. If unresolved, they have the right to complain to the **Information Commissioner's Office (ICO)**.

16. Policy Review

This policy was approved by the Academic Board in **November 2025** and will be reviewed annually or sooner if required by changes in legislation or operational practices.

Version	Date Approved	Approved by	Review Date
1.0	Nov 2025	Academic Board	Nov 2026