IIMTS
Awarding Body

IIMT STUDIES LTD
CENTRE POLICY

Data Protection Policy

Policy Compliance:
This policy complies with Ofqual,
Handbook 3.

Awarding Quality Qualifications through Global Recognition

Document Code No. **IIMTS_AO_OGCR_GDPR_01_2020**

Title of the Policy: Data Protection Policy	**Authorised by** Responsible Officer	**Created: Version 1** 1 November 2023
Conditions of Recognition: General Conditions of Recognition		**Current version: 3** **Next Review Date:** 1 April 2026

Important contact-
Any query or concern related to this policy may be directly addressed to the Data Protection Officer, the Responsible Officer or the HR Manager-

[IIMT Studies Ltd] Company
number 11649333

Registered office address
[Havelock Hub
14 Havelock Place Harrow
London HA1
1LJ
Ph- +44-7466650066

Email- info@iimtsab.co.uk
Website- www.iimtsab.co.uk

Awarding body:
IIMT Studies Ltd- www.iimtsab.co.uk

Acronym used to represent IIMT Studies Ltd (IIMT Studies):
IIMTS AB

Regulating Body:
OFQUAL
Ofqual.gov.uk

Index

(A) Policy Statement:

During our establishment and operational activities, IIMT Studies Ltd (IIMT Studies) collects and uses data about a wide range of individuals, including staff, students, candidates, and external visitors. It is essential to maintain the security and privacy of their personal data. Data protection law assures that their personal data must be kept private, maintained, processed and used in relation to its owners' rights. This policy is drafted considering the new Data Protection Act 2018 and the implementation of the EU General Data Protection Regulations 2016 ('GDPR').

IIMT Studies has policies in place, including this policy, which is designed to protect the accuracy, integrity, and confidentiality of Personal Data and ensure that individuals can exercise their rights to comply with the law.

(B) Objectives of policy:

This data protection policy ensures IIMT Studies:

- Complies with data protection law and follows good practice
- Protects the rights of employees/contractors, learners, and third-party partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of any data breach

(C) Data protection law:

The Data Protection Act 1998 describes how IIMT Studies must collect, handle and store personal information.

Data protection law applies regardless of whether data is stored electronically, on paper or in any other form of material.

In order to comply with the Data Protection Law, any information or personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The following important principles underpin the Data Protection Act. Where personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant, and not excessive
4. Be accurate and keep up to date
5. Not to be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

(D) Policy scope:

The policy applies to all employees employed by IIMT Studies, including honorary staff/associates, contractors, recognised centres, hourly paid contractors and any learners, interns or volunteers who are carrying out work on behalf of the IIMT Studies.

(E) Data protection risks:

This policy helps to protect IIMT Studies from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information is being shared out of the IIMT Studies inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

(F) Responsibilities:

Everyone who works for or with IIMT Studies has some responsibility for ensuring data is collected, stored, and handled appropriately and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that IIMT Studies meets its legal obligations.

- The **Presiding Officer** is responsible for:

    - Keeping the board updated about data protection responsibilities, risks, and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **Human Resource Manager** is responsible for:

    - Handling data protection questions from employees/third parties, and anyone else covered by this policy.
    - Dealing with individuals' requests to see the data IIMT Studies holds about them (also called 'subject access requests').

- The **IT manager / Department** is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software are functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data, for instance, cloud computing services.

- The **Marketing/PR Department** is responsible for:

    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, work with other employees/contractors to ensure marketing initiatives abide by data protection principles.

- **Data Protection Officer (DPO):**

In accordance with GDPR requirements, IIMT Studies will appoint a Data Protection Officer (DPO).

The DPO will be responsible for:

- Monitoring compliance with GDPR and internal data protection policies.
- Advising on and overseeing Data Protection Impact Assessments (DPIAs).
- Delivering training and raising staff awareness on data protection obligations.
- Acting as the primary contact for data subjects and regulatory bodies, including the Information Commissioner's Office (ICO).
- Ensuring the lawful and transparent processing of personal data.

(G) General employee/contractor guidelines:

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees/contractors can request it from their line managers or HR departments.
- **IIMT Studies will provide training** to all employees/contractors to help them understand their responsibilities when handling data.
- Employees/contractors should keep all data secure by taking sensible precautions and following the guidelines below.
- Strong passwords must be used, and they should never be shared. For any documents encrypted with a password, the password should only be shared with those for whom the data is required to be shared, and there should be a valid purpose in this instance
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees/contractors should request help from their line manager or the HR Department if they are unsure about any aspect of data protection.

(H) Data storage:

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager/ IT Department. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees/contractors should make sure paper and printouts are not left where unauthorised

people can see them, like on a printer.

- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees/contractors.
- If data is stored on removable media (like a CD or USB Drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an

approved cloud computing service.

- Servers containing personal data should be stored in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones, as they do not belong to IIMT Studies.
- All servers and computers containing data should be protected by **approved security software and a firewall**.
- Such firewalls must be approved by IIMT Studies.

(I) Data use:

Personal data is of no value to IIMT Studies. The UK, unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees/contractors should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication may not be considered secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Employees/contractors should not save copies of personal data to their own computers. Always access and update the central copy of any data.

(J) Data accuracy:

The law requires IIMT Studies. The UK, to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees/contractors who work with data to take reasonable steps to ensure it is kept as accurate and up-to-date as possible.

- Data will be held in as few places as necessary. Employees/contractors should not create any unnecessary additional data sets.
- Employees/contractors should take every opportunity to ensure data is updated, for instance, by confirming a student's details when they call.
- IIMT Studies will make it easy for data subjects to update the information IIMT Studies holds about them, for instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a student can no longer be reached on their stored telephone number or communication email addresses, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked** every six months.

(K) Subject access requests:

All individuals who are the subject of personal data held by IIMT Studies are entitled to:

- Ask what information the Institute holds about them and why.
- Ask how to gain access to it.
- Be informed on how to keep it up to date.
- Be informed about how the Institute is meeting its data protection obligations.

If the individual contacts the office requesting this information, this is called a subject access request. Subject access requests from individuals should be made in writing and addressed to the HR Department. The Department can supply a standard request form, although individuals do not have to use this.

(L) Disclosing data for other reasons:

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances, IIMT Studies will disclose the requested data. However, every step will be taken to ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where and if necessary.

(M) Providing information:

IIMT Studies aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

(N) Retention of Data:

IIMT Studies will retain personal data only for as long as is necessary to fulfil the purpose for which it was collected.

- Staff records will be retained for a minimum of **six years** after leaving IIMT Studies.
- Certain records, such as those related to tax, pensions, or references, may be retained for longer in line with statutory or business requirements.
- A Data Processing Log, maintained in accordance with Article 30 of the GDPR, will document all data retained by the organisation.

(O) Data Protection Impact Assessments (DPIAs):

IIMT Studies has established a formal process for conducting Data Protection Impact Assessments whenever new projects or data processing activities may present risks to individuals' rights and freedoms.

- DPIAs will be carried out on all relevant policies, procedures, and initiatives.
- A written DPIA report will be created and stored in a central register to ensure accountability and transparency.

This policy forms a part of a broader Governance Framework with other policies and procedures of IIMT Studies. Compliance with these is mandatory, and any breach of the requirements contained in these documents may result in disciplinary action.

IIMTS
Awarding Body

Address __

IIMT Studies LTD
Havelock Hub
14 Havelock Place
Harrow
HA1 1LJ
United Kingdom

Call us on __

+44 7466650066

Email us on __

info@iimtsab.co.uk

www.iimtsab.co.uk