



IIMTS
Awarding Body

IIMT STUDIES LTD **CENTRE POLICY**

IIMT Studies Centre Policy | Copyright- IIMT Studies Ltd. (IIMTS AB)

Information Technology (IT) and IT Security Policy

Policy Compliance:

This policy complies with
Ofqual, Handbook- General Conditions of Recognition



IIMTS

Awarding Body

Awarding Quality Qualifications through Global Recognition

Document Code No. IIMTS_AO_OGCR_AP_01_2020

Title of the Policy: IT 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 Responsible Officer or the IT Dept.-

[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

IT POLICY

Policy Code: IIMTS_AO_OGCR_IT_01_2020

Policy Statement:

This policy statement assures the secure use of IT resources made available by IIMT Studies Ltd, UK. It gives the framework within which the policy is implemented, and IT tools can be

used. It also prevents the misuse of IT infrastructure and binds users to the specified criteria mentioned in this policy. This policy applies to all employees and all stakeholders of IIMT Studies Ltd UK who use the IT infrastructure of the company.

IIMT Studies Ltd had made the IT infrastructure available for its employees for the appropriate use of their jobs and to achieve business objectives.

This policy explains the regulations governing the use of the IT infrastructure of the company. It also sets out the expected behaviour from the employees while using the infrastructure.

This policy can be read alongside the other key policy sections, such as the company's data protection and education portal process. A few components of this policy can also be read with the equality policy. The policy applies to all authorised users.

This policy applies to all IT tools, including emails, social media, the Internet, the education portal, software, Microsoft Teams version used for learning delivery and other IT tools.

Objectives of Policy: The policy aims to have a regulated IT infrastructure in place.

1. To ensure the effective use of IT
2. To protect the business interest
3. To protect the data confidentiality
4. To protect the learners' confidentiality
5. To extend the support in complex situations.
6. Ensure the users of the IT infrastructure do not violate the data protection law.

Internet use:

Section objectives:

- Minimise Internet security risks
- Listing Do's and Don'ts with the Internet
- Ensuring what employees can and cannot view
- Preventing employees from using the Internet facility for unlawful purposes
- Securing the organisation from legal obligations related to Internet usage
- Here, the Internet means the internet service provided by the organisation in the office premises, additional internet devices or internet data provided by the company's mobile connection.

The use of the Internet:

Using the Internet is a part of the business. It has to be used to support the company's objectives, communications, and purposes related to the business and follow the processes of the organisation. It can be used for the following reasons:

- Internal communication within the organisation
- External communication with enquiries and potential buyers of IIMT Studies' services

- Communication with associates and future associates who have shown interest in the services of IIMT Studies Ltd.
- Communication with learners of IIMT studies
- Performing market research
- Marketing the services and products of IIMT Studies

Personal Internet use:

The Internet is an integral part of people's daily lives. The company's internet use is allowed for personal use with the following parameters:

- The use of the Internet for personal use has to be at a reasonable level, restricted to non-working hours, such as breaks.
- While using the Internet for personal use, the user must follow all norms of this policy as they apply to the personal use of the Internet, too.
- Personal use must not be an interruption to the user's work or others' internet speed.
- Watching movies, downloading large files and downloading files from unknown sources are restricted.
- The Internet should not be used to carry out illegal acts or carry out activities that are unlawful.

Authorised users:

- Employees of the organisation
- Visitors (if authorised by the appropriate authorities)
- Learners who opt for the services of IIMT Studies can visit the

premises.

Prohibition:

- Unauthorised use of the Internet is prohibited
- The internet connection cannot be passed to any unauthorised users, and is not permitted to use the Internet

Internet security:

The use of the Internet must not create security concerns or damage IIMT Studies' data and reputation. The following must be ensured by the authorised users:

- Users must not knowingly or unknowingly download or introduce any form of internet virus that threatens the internet security of IIMT Studies. It includes, but is not limited to, Computer viruses, malware, spyware or Trojans
- Users must not download any antivirus software without permission from the IT department.
- Employees must not access unauthorised portals or websites for any purpose other than for business purposes.
- Only authorised tools by the IT department should be used to upload company data. Unknown tools are not permitted for use. It may create significant damage to the IT

security of the company.

- Use of other users' login/password, official or personal, is strictly not permitted without authorisation.

Content and use:

The following parameters must be followed while surfing the content and using the internet facility.

Prohibited use:

- Use of unauthorised content
- Any usage that puts the company's reputation at risk
- Download, create, view, forward or share inappropriate content which includes:
 - Gambling, pornography, terrorism, gender-specific comments, racial or religious slurs, illegal drugs, criminal skills and material related to cults.
- The above applies to:
 - Images, all technical formats, material, texts, videos or any other media and GIF.
- This section also includes the use of all media intending to offend someone, considering the national origin, age, sex, sexual orientation, political beliefs, race, disabilities or any protected characteristics by law.
- Use of the Internet for anti-social activities and criminal actions.
- Harassment, or communication of harassment
- Putting unsolicited views on any portal/site on religious, political, social or any matters related to non-business.

Copyright:

IIMT Studies appreciates and operates within the copyright laws. The user shouldn't use the Internet for the following matters.

- Use, download, publish or share any music, video, software, copyrighted media or media files, report, material, or documents owned by third parties, unless granted the appropriately visible permission by the owner of the brand, material, media, process, or any other format.

Monitoring use:

- Depending on your role, the company may provide laptops/desktops for the appropriate use of the internet connection. Therefore, the company reserves the right to monitor the usage, examine the system and review the data by the authorised staff.
- All data, sent, developed, shared or received through the company's IT system and infrastructure is a part of the company's record. The company holds the right to protect, monitor, and use this data as per the data protection policy.
- All users must ensure the information and data used by the internet services are accurate, appropriate, legal and ethical.

Email us:

It applies to all office email IDs or dedicated, allotted to any employee, learner, vendor or external recruitment. All component listed in Internet use (section 1) applies to the email use section. Below are the additional rules applied.

Section objectives:

- a) Minimise the business risk created by the use of email use
- b) Making the employees know how, when, and why to use the company email
- c) Ensure excellent email communication etiquette
- d) The communication should be professional
- e) Supporting the company in fulfilling legal obligations regarding the use of email

Business email use: Business emails are critical and key communication tools, and their use may be appropriate whenever used. The purposes of use are:

- Communication with customers, vendors, suppliers, contractors, learners, enquiries and potential clients of IIMT Studies services.
- Market the company's services and offers
- Sharing the authorised information with

colleagues, Personal use:

There are cases when the office email service is also used for personal purposes. If they are used for private purposes, the following should be followed.

- There should be a reasonable level of personal use and restricted to non-working hours.
- Users may use their personal email ID (use of personal email ID) during working hours, which is understandable. However, there should be a reasonable level of use of such.
 - a. Large files cannot be used if the personal ID is used through the office internet, as they reduce the overall internet speed, which may interrupt others' internet speed.
 - b. Use of personal emails should be during break hours, such as lunch and tea/coffee breaks.

User authorisation:

The user is authorised by a line manager or an authorised person in the HR or IT department. At the time of new joining, or on the requirement, the use of the existing/new email ID is authorised. People who are authorised to use the mail ID should do so. Employees must not share each other's passwords with:

- Other colleagues
- Friends and relatives
- Close relatives
- Clients

- Any third-party

Email security:

If the emails are misused, they can be a cause of security concerns and a threat to the company's confidential data. For security reasons, the following is restricted:

- a) Opening attachments from unknown sources
- b) Attachments, which may include viruses, malware, spyware or Trojan viruses, must not be opened
- c) Use of unknown antivirus software may result in data security concerns
- d) Access to the email of another user, which may result in the leak of confidential information
- e) Granting access to your email address may result in the leak of confidential information and a risk to data protection
- f) It is the users' responsibility to protect the login credentials assigned to them to avoid any misuse of their email ID and the information stored in it.

Email contents:

The company's email service must not be used to share or develop any inappropriate content. The following parameters must be followed while using the company's email facility.

Prohibited use:

- a) Use of unauthorised content
- b) Any usage that puts the company's reputation at risk
- c) Download, create, view, forward or share inappropriate content which includes: Gambling, pornography, terrorism, gender-specific comments, racial or religious slurs, illegal drugs, criminal skills and material related to cults.
- d) The above applies to:
Images, all technical formats, material, texts, videos or any other media and GIFs.
- e) This section also includes the share of all media intending to offend someone, considering the national origin, age, sex, sexual orientation, political beliefs, race, disabilities or any protected characteristics by law, using the company's email services.
- f) Use of emails for anti-social activities and criminal actions
- g) Harassment, or communication of harassment
- h) Sharing unsolicited views on any portal/site on religious, political, social or any matters related to non-business using an email ID.
- i) Abusing someone by using the company's email services.
- j) Any false commitments while purchasing, offering or selling any product or services.
- k) Purchase or sale of any product or service outside the business interest of IIMT Studies.
- l) Do not delete important emails, communications or data without proper authorisation.

Copyright:

IIMT Studies respects copyright laws. The email should not be used to share any unauthorised copyright material.

Users should keep in mind that the use of emails for forwarding/sharing copyrighted material may breach copyright.

Contracts and responsibilities:

- Users must be aware of making any commitments during purchase or offer, when using the email services.

The user must obtain proper authorisation while making any commitment to emails.

Email Disclaimer:

The user must not change or make amendments to the email disclaimer given to them by an authorised person without appropriate authorisation.

Email marketing and mass mail

Mass mail and email marketing using the company's email ID must not be done without any appropriate authorisation.

Mass emails, marketing emails or any such email communication may attract legislative law breaches.

All such emails must be sent by authorised marketing tools, authorised by an appropriate authority.

Email etiquette:

Email communication is a critical and sensitive communication tool for business. Using this tool with appropriate language and discipline is a must in order to comply with the company's policy, including this policy. The following etiquette should be followed while using this tool.

- a) Use of appropriate language
- b) Meaningful subject line
- c) Approved signatures
- d) Highlighting communications with "urgent", "important", "confidential" where appropriate
- e) Do not send Group or bulk emails, which may result in degrading the server's reputation.

Internal communication:

All employees must communicate through the company's allotted email IDs. This is an effective and secure way of communication. It leads to:

- a) Protecting confidential information

- b) Sharing the information with the authorised person
- c) Non-disclosure of confidential information

It is the user's responsibility to check who's marked as a principal recipient of the email. A wrongly marked recipient may be a severe threat and may result in copyright violation, leak of confidential information, or an unreasonable advantage to an individual, company or any identity.

Email use monitoring:

The use of email systems, software and other IT tools is provided for legitimate use to achieve business objectives. Therefore, the company reserves the right to monitor employee use of emails.

All emails received/sent are a part of the company's official records. Therefore, the company is legally responsible for showing the information to law enforcement.

It is a must for the user to keep the information received/sent through email ID, fully secured, protected, confidential, ethical, legal, appropriate and in line with the business interest of the organisation.

Email ID creation:

The brand guidelines and standard protocol were followed:

IIMT Studies has consistently followed in creating the email addresses for its employees and stakeholders. The following mechanism will be followed while creating an email ID.

- a. Management role:
(first name). (last name)@iimtsab.co.uk
For ex.: Smith Brown: smith.brown@iimtsab.co.uk
- b. Senior officers and other colleagues:
(first name). (code of geographical location)@iimtsab.co.uk For
ex.: Smith Brown: smith.uk@iimtsab.co.uk
- c. External stakeholders:
(department). (code of geographical [location](#))@iimtsab.co.uk For
ex.: hr.uk@iimtsab.co.uk

IIMT Studies reserves the right to modify and make changes to the policy. In case of a change in any policy or policy component, the amendments will be notified to stakeholders by email or any authentic communication channel.

Social media:

Section objectives:

- a) The appropriate use of social media while the employees are working, whether for personal or business purposes.
- b) It applies in all cases while working in the company premises, working from anywhere while travelling or working from home.
- c) Minimising the business risk by the use of social media sites, which include, but are not limited to:
 - Twitter, Facebook, LinkedIn
 - Social media like Instagram, Flickr
 - Use of social network sites such as Quora or Yahoo Answers for all reasons.
 - Use of social networking sites, such as education portals or popular/unpopular networking websites.

Achievement of IIMT Studies business objectives:

To achieve the organisation's objectives, the company has created social media accounts with the specified utilisation parameters. They are as follows.

- a) The authorised person, generally a social media manager, will be responsible for using the official social media account of IIMT Studies. He/she will ensure the appropriate use of social media accounts for business purposes, achieving the business goals and protecting learners' interests.
- b) The HR manager/IT manager will be authorised to allow the credentials. They are also responsible for monitoring the social media accounts and their use.
- c) The marketing team is responsible for working closely with the authorised person to use social media for approved marketing strategies.
- d) The customer service team is responsible for using social media to attend to the service concerns of stakeholders, customers and learners in case any enquiry or query falls on it.

Social media guidelines:

Today, social media is essential to stay connected with customers and stakeholders by offering marketing services or addressing their queries. The company agrees that social media is a crucial tool to learn, explore and network with excellent brains.

Therefore, the company encourages employees to use social media to support business objectives.

What to do with social media:

There are a few simple rules to follow while using social media during the company's working hours.

- a) Network understanding: Surf the FAQ before using any social media platform.
- b) Risk prediction: Do not post content if you are unsure about the reactions or consequences of sharing. You must not post any confidential information,

unauthorised data, material, video, post, image or any form of document unless authorised to do so.

- c) Language: Use professional language while posting anything on social media. Do not sound negative on social media. There is a thin line between sounding critical and negative.
- d) Security alerts: The user mustn't use social media platforms which cause security threats either for a person's or a company's information.
- e) Personal use: The personal use of social media during working hours should be reasonable.
- f) Making promises: Do not make promises/commitments on social media on behalf of IIMT Studies Ltd. The user may forward the enquiry/query to the appropriate authority to handle it.
- g) Use of other channels: All queries/concerns may not be used on social media. Use different channels for complex queries. The user should keep the practice of forwarding all questions to the appropriate department for further action.
- h) Quick response: Try responding quickly on social media. This creates a better version of an impression if any stakeholder has used social media.

Authorised use:

- a) Users who are authorised to use the accounts should use the social media accounts.

Creating accounts:

- a) It is essential to gain appropriate permission before opening a new social media account using the company's brand image, for example, the logo. There is a limitation on creating multiple social media accounts for the company.
- b) Social media managers may help if there is any enquiry about opening a new social media account or using the existing one for any permitted purpose.

Why social media accounts:

There are reasons to open a social media account. It is open to support business goals. It includes:

- a) Attending to customer queries.
- b) Sharing blogs and articles developed by IIMT Studies
- c) Marketing the product/services as per the approved marketing strategies
- d) Share approved images, videos and other media content in the public interest.
- e) Making social offers or announcements.

Share of content:

The company's social media accounts must not be used to share or develop any inappropriate content. The following parameters must be followed while using social media services.

Prohibited use:

- Use of unauthorised content
- Any usage that puts the company's reputation at risk
- Download, create, view, forward or share inappropriate content which includes:
- Gambling, pornography, terrorism, gender-specific comments, racial or religious slurs, illegal drugs, criminal skills and material related to cults.
- The above applies to:
- Images, all technical formats, material, texts, videos or any other media and GIFs.
- This section also includes the share of all media intending to offend someone, considering the national origin, age, sex, sexual orientation, political beliefs, race, disabilities or any protected characteristics by law, using the company's social media account.
- Use of emails for anti-social activities and criminal actions
- Harassment, or communication of harassment
- To share unsolicited views on any portal/site on religious, political, social or any matters related to non-business using email ID.
- Abusing someone by using the company's email services.
- Any false commitments while purchasing, offering or selling any product or services.
- Purchase or sale of any product or service outside the business interest of IIMT Studies.
- Do not delete important emails, communications or data without proper authorisation.
- Official communication with colleagues which requires record-keeping
- Discussion about colleagues, competitors or vendors.
- Disclose any confidential information, links or material.
- Any act which can potentially defame IIMT Studies or damage its brand image.
- Any hate speech, negative talk or comment, rude, disrespectful or offensive statement.
- Share the data that can breach the data protection policy.

Use:

- a) Social media, for work purposes, can be used for a specific reason. However, it should not interrupt the regular duties of employees.
- b) Any use for non-work purposes is allowed only during break times.
- c) The employee should ensure that their posts, comments or accounts do not represent IIMT Studies Ltd's views or opinions.
- d) Employees may wish to keep the disclaimer in their accounts: "The views and opinions are personal."
- e) The rules are applied to any employee using a company social media account and any employee using a personal social media account during working hours.

Copyright:

IIMT Studies respects copyright laws. Social media accounts should not be used to share any unauthorised copyright material.

Users should keep in mind that the use of social media for forwarding/sharing copyrighted material may breach copyright.

Protect account:

- a) The user must protect the company's social media account by keeping a strong and reasonably complicated password.
- b) The user must not use their personal credentials to create any social media account which is to be used for business activities.
- c) The user should enable two-factor authentication.

The account handover:

- a) The account must be handed over to the respective authority with all credentials in case of the end of employment or termination.

Monitoring the account:

The use of the company's social media accounts, email system, software and other IT tools is provided for legitimate use to achieve business objectives. Therefore, the company reserves the right to monitor employee use of IT tools provided by the company, including emails received/sent, which are a part of the company's official records. Therefore, the company is legally responsible for showing the information to law enforcement.

It is unnecessary for the user to keep the information received/sent through social media fully secured, protected, confidential, ethical, legal, appropriate and in line with the business interest of the organisation.

Policy disclaimer:

Breaching this IT/Information security policy is a serious matter which may lead to disciplinary action, including termination of the contract, employment or registration.



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