INSTITUTE OF TOURISM STUDIES
IN ACADEMIC AFFILIATION WITH THE EMIRATES ACADEMY OF HOSPITALITY MANAGEMENT

EMAIL & INTERNET USE

CODE: P009

Section: ICT
Policy Owner: BOG
Procedure Owner: ICT DEPARTMENT

Last Reviewed: January 2021

COMPUTER SYSTEMS POLICIES AND PROCEDURES

1.0 Scope

1.1 The aim of this policy is to provide guidance in the effective use of the ITS connectivity and electronic communication tools, to support the activities of the institution that include learning, teaching, research and administration. This policy has been developed to enable and encourage the exchange of electronic forms of information in a controlled and secure way.

1.2 The term network, and references to it throughout this document, covers the use of any local area network within the ITS, as well as access the Internet and other networks using ITS equipment. It includes all connections types, whether wired or wireless and all related systems and equipment.

1.3 All staff, students and associate members of the ITS who have been granted authorised access to the ITS network, must abide by these policies, the Institute's rules and regulations and the terms and conditions set out.

Supplementary information regarding authorised access to the ITS network can be found in the ITS Network Policy.

2.0 The Use of Computers at Work

2.1 The ITS's computers are provided to support learning, teaching, research and administrative activities in the institution. Access is only permitted through an authorised ITS account, which is necessary to provide an audit trail of user activity on the network. At its own discretion, the ICT Department might provide a limited guest access on some systems.

2.2 Staff and students who are authorised to access resources through the ITS network should be inducted to ensure that ITS network policies are known and are understood. Any staff and students found in breach of these guidelines may be subject to ITS disciplinary procedures. While the ITS will strive to ensure that all users are made aware of its policies, regulations, rules and T&Cs, it is ultimately the responsibility of the users to ensure that they have read, understood and are compliant with these policies and regulations.

2.3 Any software installed, used or accessed in any way on ITS devices and through ITS network and/or systems must be approved by the ICT Department prior to its installation/use. A formal request for the use/installation of such software must be made to the ICT Manager following approval for such use by the Users' Head

of Department and/or representatives thereof. The ICT Department might, at its own discretion, refuse the installation/use of any software it deems harmful, unnecessary or for which no right justification has been submitted, irrespective of any approval obtained at Departmental level.

2.4 All ITS corporate devices will be locked with Administrator passwords to help minimise the risk of virus infection that may have a damaging effect on the operation of ITS' systems, as well as to avoid the use of illegal, illicit or destructive software.

2.5 It is an offence for users to misuse the ITS's computer systems and networks, as per applicable Maltese legislation and other policies, rules and regulations issued by the Institute, the country, the EU and or international authorities. Examples of such misuse may include, without being limited to:

i. Accessing an ITS system or network without authority;
ii. Using a username/password that belongs to another user, student or member of staff;
iii. Using shared passwords;
iv. Sending e-mail(s) to large groups of individuals when this has not been formally authorised;
v. Accessing commercial or personal data when not authorised to do so or for a purpose otherwise than in connection with an individual's duties for/within the ITS;
vi. Installing and using non-approved software, which is software that has not been installed or approved by the ICT Department;
vii. Installing and using non-licensed software;
viii. Installing and using non-approved hardware;
ix. Unauthorised copying and distribution of electronic copyright material;
x. Unauthorised running of commands or programs that have the potential to affect systems performance or accessibility.
xi. Intentional spreading of malicious, illicit and/or illegal software
xii. Engagement in behaviour that is offensive, harassing, illegal, malicious or otherwise harmful to other users or ITS systems, that damages the ITS brand and its products or reputation at any level.

3.0 E-Mail Policy

This section governs the use of the ITS's e-mail system, to facilitate the exchange of electronic information both internally and externally to the organisation. E-mail systems, provided as part of the Institute's ICT Services, are modelled in the full respect of the GMICT policies and other applicable policies, rules and regulations. Third party e-mail systems provided to ITS by private organisations are governed by this Policy.

It is important to note that the ITS staff and student e-mail systems are key communications systems in the Institution. Inappropriate use of the e-mail systems can have myriad consequences that vary from infection and dissemination of malware (virus infection, ransomware) to loss of data and/or data theft (phishing) to software and/or hardware damages among others. These could ultimately lead to a degradation of network performance, or in extreme circumstances take the whole of the ITS network down. The use of ITS email (and other communication systems) can have personal, professional and legal consequences.

3.1 Computer Malware: Incoming e-mails and their attachments may carry dangerous or potentially business damaging malware. If an individual is in any doubt about the contents of an e-mail message and suspects the existence of a such malware they should not open it, but must consult the ICT Department immediately to obtain technical assistance. In relation to outgoing e-mails, staff or students may be held liable if e-mails containing harmful content such as computer viruses, are sent either internally or externally. If there is any doubt regarding e-mail attachments, the ICT Department should be contacted immediately.

3.2 Offensive or obscene e-mail: If there is any reason to suspect that an incoming e-mail may contain offensive or obscene material, where possible, refrain from opening it. Under no circumstances should the e-mail be sent on to another user, and it should be reported to the ICT Department immediately. Pornographic or other any offensive materials that contravene ITS policy or Maltese and European legislation, should not be sent at any time to any users, and their dissemination might carry liability and disciplinary consequences.

3.3 Confidentiality: While ITS strives to ensure high standards of data protection and safety, users should avoid sending sensitive and personal data (such as, but not limited to, banking details, passwords, personal data, etc.) via email without the proper encryption and security measures taken as needed. Personal data should not be shared without the owners' consent. Attachments containing sensitive information should be password protected or encrypted.

3.3.1 Personal e-mail messages may be open to scrutiny without an individual's permission. For example, the ICT Department in the course of their duties may have to investigate the contents of e-mail which has been delivered to an unknown e-mail address.

3.3.2 All outgoing e-mails should contain the sender's name, title and contact information using the standard ITS email signature block

3.4 Content: All users should treat emails as formal communication content representing ITS and should at all times ensure that they are using the correct email signature and following the correct branding guidelines, as directed by the Marketing

Department and Executive Management. Any digressions from the corporate branding guidelines and corporate communication guidelines will be reset.

3.4.1 E-mail is accepted in law as evidence and therefore legislation relating to Data Protection and Intellectual Property applies equally to e-mail messages, so the same care should be given to the tone and content of e-mails, as for paper communication.

3.5 Checking e-mail/Out-Of-Office: ITS mailboxes should be checked regularly, and messages answered in a timely manner, in accordance with Departmental or Organisational SLA with customers (internal and/or external).

3.5.1 If a user is going is not going to be in the ITS to respond to their e-mails for an extended period of time, then they should either: Authorise or delegate access to another staff member of staff to check the e-mails on their behalf; or b) arrange to access their email remotely (given authorisation by management).

3.5.2 Email users who are away from their inboxes should always set-up 'out of office' messages to advise clients that their messages might not be attended to in a timely manner. The guidelines for wording and formatting these Out-Of-Office Messages are provided by the Marketing Department or by Management and should equally follow content rule as much as any other email.

3.5.3 All suspicious mail content that is not caught by the ITS Spam filter mail should be reported immediately to the ICT department such that any safety measures than can be taken are taken and/or enhanced.

3.6 Printing e-mails: Users should limit the printing of unnecessary documents, in particular emails. However, from time to time it may be necessary to obtain a hard copy of appropriate e-mails to record an audit trail for relevant ITS business. All rules and regulations that apply to digital content (especially, without being limited to, data security and data protection) must also apply to all printed material.

3.7 Unnecessary Messages: Users should avoid as much as possible situations where bulk emails are sent to multiple recipients, as well as the sending of large trivial messages, or unnecessary e-mail messages. Staff and students are required to ensure that:

3.7.1 Bulk E-mails are not to be circulated without the express consent of the ICT manager.

3.7.2 E-mails are kept as short and accurate as possible.

3.7.3 Sending of large attachments should be avoided and alternative facilities (one-drive, sharepoint, online-transfer services) should be used when needed.

3.8 Personal Use: The ITS allows the limited personal use of the e-mail system/s officially in use at the Institute, provided that such personal use does not interfere with the main business activities of the institution, and does not jeopardise the effective operation of the ITS' systems and services. Personal use of ITS systems (including emails) are subject to the same regulations, frameworks, policies, laws and conditions as professional/corporate emails are subject to, and carry the same liabilities.

3.9 Unauthorised Use: The ITS will not tolerate the misuse of the e-mail system. The following are examples that are considered a misuse of the system:
Any message that could constitute bullying or harassment (e.g. on the grounds of sexuality, race, disability or age) or that could be considered offensive, obscene or in bad taste;

a. Any message that could constitute defamation, for example in relation to other students, or members of staff within the ITS;
b. Persistent unauthorised personal use, including but not limited to personal messages, social invitations, jokes, cartoons or chain letters;
c. On line gambling;
d. Accessing, circulating, distributing or otherwise publishing pornography internally within the ITS or externally;
e. Sending or distributing copyright information and/or any software available to the user;
f. Posting confidential information about other students, staff members, the ITS or its suppliers;
g. Sending of unsolicited e-mail to internal or external recipients;

E-Mail Etiquette: The ITS will regularly inform users of expected etiquette, branding and style. Users are therefore required to adhere to such directions, as made available by management.

4.0 Internet Policy

The main aim of this policy is to provide advice and guidance to create a safe and secure environment for staff and students to undertake ITS business over the Internet.

Using the Internet for any illegal activity, including violation of copyright or other legal rights, the unauthorised transmission or receipt of proprietary information, or transmitting any material that is in breach of Maltese or European legislation, is not allowed. In addition, the Internet should not be used for the transmission of, retrieving, observing or storing of any communication that is:

i. Discriminatory or harassing in any sense whatsoever and whether prohibited by the law or not;
ii. Pornographic or derogatory to any individual or group;
iii. Involves accessing entertainment, sport or gambling websites or other websites which have no legitimate connection to the ITS' business;
iv. Defamatory or threatening, whether legally actionable or not;
v. Illegal or contrary to the ITS' policies or business interests;

Under 18-year-olds may be asked to provide written consent of a parent or legal guardian to their access of Internet through ITS computers. All users must agree to abide by the ITS Internet & E-mail policy.

A degree of filtering can be applied to all designated child accounts. However, it should be noted that whilst every effort will be made to block access to illegal and 'undesirable' sites, filtering technology cannot block all offensive sites. Therefore, ITS cannot guarantee that users will not accidentally access information and/or images that individuals may find offensive or disturbing.

4.1 Personal Use: The ITS allows the limited personal use of the Internet, provided that such personal access does not interfere with the main business activities of the institution and does not jeopardise the effective operation of the ITS' systems and services. In any case, such personal use shall not, in any way, constitute a breach of all applicable policies, rules, regulations and laws this Policy is subservient to.

4.2 Personal Privacy and Monitoring: The ITS assumes that its staff and students will act in a reasonable manner and adhere to the highest standards of conduct in the use of ICT Systems. The ITS maintains a full audit trail of activity under normal circumstances. However, the ITS reserves the right to monitor activity to ensure that the systems are being used for legitimate business purposes including the following:

a. To ensure compliance from time to time with the ITS Email & Internet Use Policy
b. To prevent or detect the unauthorised disclosure of any information which is confidential to the ITS. For these purposes, any information held within the ITS's Systems is to be treated as being confidential unless the ITS has taken active steps to publish the information. Confidential information includes details of the ITS's students, suppliers, employees, financial or trading results, and any details relating to the ITS's services.

4.3 The ITS reserves the right to monitor patterns of computer use, websites accessed, connection lengths and times at which connections are made. These may be monitored for legitimate purposes, including – without being limited to:
a. Cost analysis and Resource allocation;

b. Optimum technical management of information resources;
c. Detecting patterns of use that indicate students or staff members are violating ITS policies or engaging in unauthorised activities.

4.4 The ITS reserves the right at its discretion, to review the electronic files and messages of any user of the ITS- supported Internet connection.

4.5 Safeguarding Access to Workstations: Workstations should not be left unattended as this provides an opportunity for others to access the e- mail system and send items in your name. Users must always lock their devices when these are left unattended. Where possible, the ICT Department will enforce an automated device locking system. It is however the responsibility of the users to ensure that their devices are kept safe; to avoid unauthorised/unattended access and secure any data they might be in possession of.

4.6 Usernames & Passwords: All network users are issued with a unique username and password which is changed at regular intervals and is confidential to the user. However, it may be required at times for users to disclose their passwords to authorised the ICT Department staff, to help ensure compliance with ITS policy and maintain the integrity of ITS computer system