Subject:	IT USE POLICY FOR STUDENTS		
Version:	V4-210323	Supersedes:	V3-200723

This document is issued and controlled by the Quality Manager. Approval for changes may only be given by the Director or in his/her absence, a nominee appointed by the Director. This is a controlled electronic document, is subject to updates and must not be copied.

Contents

Target Group:	Middlesex University Dubai students and alumnus
Category:	IT Policies
Created/Reviewed by:	Quality Office
Approved by:	Pro-Vice Chancellor & Director, Dr Cedwyn Fernandes
Date:	March 2021

1. INTRODUCTION

This policy is part of our University's commitment to supporting our students to enable them to achieve their full potential. This Policy is prepared for all students of the University or alumnus, together referred to as "**Users**". The University requires all Users to comply with this policy when using the University's computers, network and other associated IT services.

This Policy explains:

- how Users may use the University's IT facilities;
- how Users or the University may be liable in law for misuse of the University's IT facilities;
- how User's interests and the University's interests can be protected;
- the action which may be taken against Users if you fail to comply with the rules and regulations set out in this Policy; and
- details of the email and file storage services provided by Microsoft.

2. DEFINITION AND SCOPE

The University encourages all Users to use the University's IT facilities as tools to assist their studies and work. All the computers, IT equipment and software at the University, especially those in the Computer Labs and the Library are provided for use in furtherance of the mission of the University and for your academic benefit. Only Middlesex University Dubai students are allowed to use University facilities, studios, computer laboratories (labs) and IT facilities in addition to authorised staff members, alumnus and campus visitors.

This Policy applies to all computer users within the University (including persons who are not staff or students but who have been authorised in writing by University to use the University's IT facilities), whether they use computers based at the University's premises or access the systems provided by the University via the internet using University-owned or private IT equipment. Compliance with this Policy does not imply authorisation to use the University's IT facilities.

You hereby agree to use the Middlesex Student Office365 and OneDrive facilities (together, the "**Microsoft Facilities**") as provided by Microsoft on behalf of the University in accordance with these terms and conditions and you hereby agree that you are also bound by Microsoft's 'Terms Of Use' which can be read by clicking here https://www.microsoft.com/en-us/legal/intellectualproperty/copyright/default.aspx.

The University reserves the right to amend any of the rules set out in this Policy at any time, and will notify all Users of any changes it makes.

In accordance with the University's 'Regulations' (which can be read by clicking here https://www.mdx.ac.uk/about-us/policies/university-regulations), the University considers failure or refusal to comply with this Policy to be a serious disciplinary offence which may lead to disciplinary action including, without limitation, withdrawal of services and/or expulsion (with or without notice) in accordance with the following parts of the University Regulations:

- Academic-Integrity-and-Misconduct
- Student-Conduct-and-Discipline-Rules
- Student-Complaints-and-Grievance-Procedures
- Appeal-Regulations-and-Procedures
- Student responsibilities

Comprehensive policies govern usage of IT facilities (including IT facilities, email and the Internet) at Middlesex University. For more information see: https://unihub.mdx.ac.uk/student-life/important-documents/policies

At all times, students must also ensure full compliance with the laws of the United Arab Emirates (UAE). This includes the regulatory framework of the Dubai Government's Knowledge and Human Development Authority (KHDA), Dubai Development Authority (DDA) and all other applicable federal or Emirate-level laws. The United Arab Emirates has several laws (for example, Federal Law No. 5 of 2012 on Combatting Cybercrimes and its amendment by the Federal Law No. 12 of 2016) for the protection of privacy and reputation and defamation. The UAE laws and resolutions concerning activities conducted online can be found on https://u.ae/en/resources/laws.

3. IT USAGE

The University's IT facilities are provided to assist with day to day work or studies. Personal and recreational use is allowed; however, the University accepts no responsibility for personal data stored on devices or storage facilities. The University also reserves the right to place whatever limitations it deems appropriate on such usage in order to safeguard the function of its IT facilities and Users' compliance with any applicable laws and/or the contents of this Policy.

When using the University's IT facilities Users must conduct themselves at all times, in a lawful and appropriate manner so as not to discredit or harm the University or other Users and at all times in accordance with the contents of this Policy. Accordingly, this Policy is not

a definitive statement of the purposes for which the University's IT facilities should or should not be used and the University reserves the right to apply this Policy in a purposive manner.

At all times, students must also ensure full compliance with the laws of the United Arab Emirates (UAE). This includes the regulatory framework of the Dubai Government's Knowledge and Human Development Authority (KHDA), Dubai Development Authority (DDA) and all other applicable federal or Emirate-level laws.

These facilities are not designed as entertainment or recreational areas. Students may not download music or video files, nor may they install computer games or other personal software or change any of the computer settings, unless these are part of academic requirements and they receive formal approval from the University IT Manager.

4. IT RULES & REGULATIONS

4.1 BASIC RULES

- Only use the University's IT facilities for lawful activities. Do not engage in any activity or omit to do anything which could jeopardise the integrity or security of the University's IT facilities.
- Keep your 'Network Identity', all your User 'Accounts' and associated passwords secure.
- Do not share your own or use someone else's 'Network Identity' and User Account (even with the owner's permission).
- Do not bypass the login procedure.
- Do not use, or permit others to use, the University's IT network for any commercial use, nor for the purposes of endorsing or advertising such activity without the express authority of the University's IT Department.
- Do not copy, rename, change, examine or delete files or information belonging to some other user or to the University.
- Copying or transferring any computer software and hardware provided by Middlesex is not permitted under any circumstances.
- Do not access material, or attempt to access material, that you do not have permission to access.
- Do not deny (or do anything which has the effect of denying) another Users' legitimate access to the University's IT facilities.
- Do not send unsolicited bulk email messages, chain mail or spam.
- Do not attempt to modify system facilities, illegally obtain extra resources, degrade the performance of any system, or attempt to subvert the restrictions associated

with any computer system, computer account, network service or micro-computer software protection.

- Do not connect any server, modem, wireless routers and hubs or network routers / switches / hubs to the University's computer network, or other similar transmitting device that operates on a wireless frequency without prior written agreement from the IT Office.
- You may not remove any equipment or materials from the computer labs without authorisation. Failure to observe this may lead to the suspension of access to IT facilities and action within the University's disciplinary procedures.
- It is **strictly forbidden** to disconnect any computer cables (network, mouse, keyboard, monitor, power) from the library / computer lab computers and from the power supply (both monitor and computer power supply cables). **Do NOT unplug the network cable from the university computers**.
- Data points provided for Users are designed to support one computer only and the unauthorised connection of hubs and switches to data points is forbidden.
- Do not deliberately or recklessly undertake activities which may result in any of the following:
    - The waste of staff effort or network resources, including time on any system accessible via the University network
    - The corruption or disruption of other User's data
    - The violation of the privacy of other Users
    - The disruption of the work of other Users
    - The introduction or transmission of a virus into the network

4.2 BASIC LAB RULES

- Before entering a computer lab, you should check whether a 'Do not enter' notice has been posted on the door(s) to the room. If there is such a notice, do not enter the room. If you are working in a computer lab prior to the start of a scheduled class/workshop, you may have to make way for the scheduled class. If asked to leave the room, you should do so promptly and politely.
- Please make sure you carry your Student ID Cards at all times.
- You must make sure that your belongings are not left unattended. The University is not responsible for any loss or damage to student personal belongings.
- No food or beverages are allowed in the library or the computer labs. **Smoking in the labs is strictly prohibited**. Skating, running and similar activities are prohibited for safety reasons. Noise in general should be kept to a minimum. Please respect those studying within the same area.
- Mobile phones must be on silent. No conversations may take place on mobile phones in the computer labs. Messages may not be listened to on mobile phone in

the computer labs. No devices (laptop, tablet, phone, etc.) may generate noise. Headphones must be used with all devices that are noise-producing.

4.3 UNAUTHORISED USE OF THE INTERNET

- The University equipment should not be used for any illegal activities. Copying/ downloading/ sharing/ playing pirated media is strictly forbidden.
- Chat software, movie streaming services and online gaming are restricted as they use significant amount of bandwidth which may hinder the academic needs of other users. Instant messaging and gaming are restricted on the lab computers.
- Do not visit, view, store, download, transmit, display, print or distribute any material relating to:
    - Sex or pornography;
    - Lewd or obscene material of any nature or other material which may be likely to cause offence to another person;
    - Terrorism or cults;
    - Hate sites (racial or other).
- In addition, Users should not intentionally do anything which enables others to visit, view, download transmit, display, or distribute any material relating to the items listed above.
- Do not attempt to gain unauthorised access to any facility or service within or outside the University, or make any attempt to disrupt or impair such a service.
- Do not set up or use hardware, or software, on the University's own internal network for the purpose of sniffing, hacking, network scanning or keyboard logging without prior written authorization.
- Do not alter or interfere with data, programs, files, electronic mail or other computer material which you do not have the right to alter.

4.4 NEWS AND COMMUNITY GROUPS, WEB SITES, WIKIS, BLOGS:

- Do not post or present information in such a way as may bring the University into disrepute or otherwise damage the reputation of the University.
- Do not express opinions which purport to be the University's view unless you are authorised in writing to express views on behalf of the University.
- Do not distribute or share group members' user names, email addresses and other personal information with non-group members.
- The University reserves the right to approve and withdraw approval of any News and Community Group, Web Site, Wiki and Blog.

4.5 EMAIL

- The University encourages Users to use email as a prompt and effective method of communication.

- Email services are provided to Users through the use of Microsoft's Facilities.
- Users must act responsibly and appropriately when using the University's IT facilities to send email**,** whether internally or externally using the Internet.
- Users must not send email which might bring the University into disrepute or purport to be the view(s) of the University unless the User is authorised in writing to express views on behalf of the University.
- No User should send email that contains material that the University considers or might reasonably be considered by the recipient as offensive, (including without limitation bullying, harassing, discriminatory, pornographic, homophobic, excessively violent, obscene, blasphemous, seditious, incite racial hatred), defamatory or in any way break any law relating to published material or which contains any malicious code; for example, a virus. If you receive an email containing any such material, and you are concerned about this you should contact Help Desk at Helpdesk@mdx.ac.ae.
- The University and the University on behalf of its externally hosted providers, including Microsoft, reserves the right to automatically delete emails which are found to contain viruses or constitute a data security breach (e.g. contain sensitive and or authentication cardholder data). The University endeavours to protect Users from offensive emails through the operation of 'Anti-Spam filters' (as part of the Microsoft Facilities) PROVIDED THAT in addition, Users endeavour to reduce the amount of offensive material they receive by the configuration of their email setup to screen out and delete unwanted emails.
- Users hereby agree that emails generated by, or stored on, the University's computers or the University's externally hosted computers (including Microsoft Facilities) may be subject to disclosure under the Freedom of Information Act and Data Protection Act as well as potentially disclosable and admissible in evidence, in a dispute.
- The students can access the University email service up to a year post graduation. We recommend students to inform all contacts of their change of email address to their personal email.

4.6 SOFTWARE

- *Unauthorised Software:*
    - The University will take disciplinary action against any User who acquires, uses or distributes unauthorised copies of any software using the University's IT facilities.
    - The download and installation of malicious software is forbidden and is considered as a violation of University regulations even when unintentional.
    - Computer facilities should not be used to violate the terms of any software license agreements, or copyright provisions.

- Do not make, store or transmit unlicensed copies of any trade mark or copyrighted work (including software and media files).

- *Introducing Software:*
  - Users are prohibited from using any software on the University's IT facilities which the User and/or the University is not licensed to use.

- *Educational Use Licences:*
  - The University licenses computer software from a variety of outside sources and many software packages are licensed only for educational use. The University does not own this software or related documentation and, unless authorised by the software owner, does not have the right to reproduce it.
  - The software used on the local area network or multiple/individual machines may only be used in accordance with the relevant licence agreement and in no circumstances for any commercial use without the express authorisation of the IT Office.

- *Distribution of Software:*
  - Users are prohibited from using the University's IT facilities to distribute software unless (and not without the University's express written approval) it is directly associated with the University's business and where such distribution does not contravene any other part of this Policy.

- *Suspected Misuse:*
  - Users should immediately notify the IT Office of any misuse or suspected misuse of software or associated documentation.

- *Deep Freeze software:*
  - All the University computers run the **Deep Freeze** software. Restarting the computer makes it go back to the original state meaning that work saved anywhere except your Home Drive (G drive in My Computer) or My Documents, personal flash disks, USBs or portable storage devices will be lost. You can also e-mail your work to your private e-mails or UK e-mail accounts. Lecturers are informed about the Deep Freeze software therefore students cannot use it as an excuse for any lost work (especially on the day of submissions).

4.7 ONLINE PLAGIARISM AND ONLINE PURCHASING OF ASSIGNMENTS

- The University is aware of online plagiarism and that sites exist where it is possible to purchase assignments. Users hereby acknowledge and agree that the University actively monitors Internet use and submitted assignments for evidence of plagiarism.
- Any abuse or evidence of plagiarism is considered to be a serious offence, and will be dealt with under the academic misconduct procedures in section F of the Regulations.
- You must comply with all intellectual property, data protection and copyright laws, and related University regulations.

4.8 SECURITY AND VIRUSES

- It is each User's responsibility to log off from the system when leaving the computer being used to avoid inadvertent security breaches.
- Users must not disclose (including by sending via or placing on the Internet) any material, which incites or encourages or enables others to gain unauthorised access to the University's computer facilities.
- It is vital that all Users take all necessary steps to safeguard the University's computer facilities from viruses. Accordingly, all Users using personal computers on the University system must ensure that anti-virus software is installed on their desktop / laptop computer and kept up to date and that any unsolicited documents or attachments received are deleted immediately.

4.8 OFFENSIVE OR DEFAMATORY MATERIAL

- Emails and the Internet are considered to be a form of publication and therefore the use of the Internet, email and the making available of any information online, must not be offensive, (including without limitation bullying, harassing, discriminatory, pornographic, homophobic, excessively violent, obscene, blasphemous, seditious, incite racial hatred), defamatory or in any way break any law relating to published material.
- Misuse of email or inappropriate use of the Internet by viewing, accessing, transmitting or downloading any such offensive information will amount to a serious offence and/or gross misconduct pursuant to the Regulations and may result in withdrawal of services, expulsion or any other penalties as set forth in the Regulations.
- Words and pictures produced on the Internet are capable of being defamatory if, for instance, they are untrue, ridicule a person and as a result damage that person's reputation. For these purposes, as well as any individuals, a "person" may include the University or another institution.
- You must not create or transmit any statement which may be offensive or defamatory in the course of using the Internet or the University's IT facilities

whether in emails or otherwise. As well as you being personally exposed to potential legal action for defamation, the University and would also be held liable.

4.9 OBSCENITY

- It is a criminal offence to publish or distribute obscene material or to display indecent material in public. The Internet or any computer 'message boards' qualify as a public place.
- The accessing or sending of obscene or indecent material using the University's IT facilities is strictly forbidden and in accordance with the Regulations may result in withdrawal of services or expulsion.

4.10 DISCRIMINATION AND HARASSMENT

- The University does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed on the University's IT facilities or via the Internet. Users should not view, use or distribute any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, gender reassignment, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability.

4.11 DATA PROTECTION

- Any work involving processing, storing or recording personal data (information on an identifiable living individual) is governed by the Data Protection Act 2018. It is the User's responsibility to ensure that personal data is collected and used in accordance with the Act. Further information can be obtained from the University's Data Protection Policy.

4.12 MONITORING

- The University reserves the right without notice to monitor Users' use of the University's IT facilities and to access data held on the University's ITIT facilities for justifiable business purposes and in order to perform various legal obligations including:
    - where it is suspected that a User is misusing the University's IT facilities;
    - to investigate misuse of the University's IT facilities;
    - where the University has received a request from an authorised external party to monitor a User's use of the University's IT facilities;
    - to prevent or detect crime (including 'hacking');
    - to prevent or detect data security breaches;
    - to resolve system performance problems which may otherwise damage the IT services provided to other University users; or

  - to intercept emails for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding emails to correct destinations.
- The University reserves the right to automatically block certain network protocols and sites in order to minimise the risk of viruses, hacking, network scanning and other inappropriate file transfer activities.
- The University maintains logs of user and network activity which may be used in investigations of breaches of University IT regulations, performance monitoring or provision of statistical reports.
- The University reserves the right to make and keep copies of emails and data documenting use of email and/or the Internet systems, for the purposes set out above.
- Users hereby acknowledge and agree that the University has the right to retain copies or delete copies of any data stored on the system so as to comply with the University's statutory obligations or, at its own discretion, in accordance with the legitimate purposes stated above.
- In using the University's IT facilities, Users implicitly accept this Policy. Consequently, Users agree to their activities being monitored in the circumstances given above.
- The University Student Network is being monitored by a firewall which prevents the download of music and videos due to international copyright laws. P2P network applications are restricted. Voice over IP (VoIP) telephony applications are blocked in accordance with the UAE Telecommunication Regulatory Authority (TRA) laws. Web sites which are banned or otherwise deemed offensive to the local culture and traditions by the TRA are also banned.
- There are security cameras in the library and computer labs.

4.13 AVAILABILITY

- Users acknowledge that the University's IT facilities may not be available for 24 hours 7 days a week. Lab availability is restricted from 08:00 till 22:00 all 7 days a week. If students want to use the labs beyond these timings, they will have to get a written approval from the CPC of their programme and the IT Manager.
- The University retains the right to limit or prevent access to the University's IT facilities for the purposes of carrying out planned or unplanned maintenance, virus monitoring and/or clean up or investigation.
- Except where the University cannot exclude or limit its liability as a matter of law, the University shall have no liability to any User in connection with the non-availability of the University's IT facilities howsoever arising, including in negligence.

4.14 LIABILITY FOR MISUSE AND DISCIPLINARY ACTION

- Misuse of the University's IT facilities (including failing to comply with this Policy) may expose both Users personally and/or the University to court proceedings attracting both criminal and civil liability. Users will be held responsible for any claims brought against the University for any legal action to which the University is, or might be, exposed as a result of User's misuse of the University's IT facilities including reimbursing the University for any financial liability which the University suffers as a result of Users actions or omissions.
- The University considers failure or refusal to comply with this Policy to be a serious disciplinary offence which may, in accordance with the Regulations, lead to disciplinary action taken including withdrawal of services and/or expulsion with or without notice. Action (including certain penalties) may be taken under the 'Student Conduct and Discipline' section contained within the Regulations.
- Users acknowledge that it is their own responsibility to create and maintain 'back-ups' of any data. The back-ups taken by the University are used for systems recovery purposes. Users hereby acknowledge and agree that it is not possible to recover any emails and files held on the Microsoft Facilities.
- Students found damaging IT property, stealing, or defacing IT equipment, software or spaces will be subject to University disciplinary procedures including fines and charges for replacement of property.
- All those in breach of the above regulations will be asked to leave the computer lab and/or the Library and/or the University premises. Additionally, their Student ID cards will be confiscated. This will be regarded as a violation of the Student Code of Conduct and action will be taken under the University's disciplinary procedures.
- *The University's Liability to Users:*
    - The University does not exclude its liability under this Policy (if any) to Users:
    - for personal injury or death resulting from the University's negligence;
    - for any matter which it would be illegal for the University to exclude or to attempt to exclude its liability; or
    - for fraudulent misrepresentation.
- Except as provided above, the University will be under no liability to Users whatsoever (whether in contract, tort (including negligence), breach of statutory duty, restitution or otherwise) for any injury, death, damage or direct, indirect or consequential loss (all three of which terms include, without limitation, pure economic loss, loss of profits, loss of business, loss of data, loss of opportunity, depletion of goodwill and like loss) howsoever caused arising out of or in connection the use of the University's IT facilities.

5. REVIEW

The policy will be reviewed at least every year.

6. RECORD KEEPING

The Quality Office will be responsible for record keeping and keeping track of changes made to the policy. These will be documented as indicated in the table below.

Amendment History

Previous Version	Changes to previous version in the current version and date.	Updated by	Authorised by
V3-200723	Title of the policy changed to IT Use Policy for Students-MDX-DBI Major changes made to the policy, based on the Hendon policy	Quality Manager	Director
V2-190521	No major changes made, Title remains MDX IT Rules and Regulations	Quality Manager	Director