Acceptable Usage Policy (Student)

Author	Arthur Bogacki
Date	18/10/2017
Version	1.1 (content sourced and consolidated from existing Email and Electronic Communication, and User Code of Practice policies.)
Review requirements	Within two years
Date of next review	18/10/2019
Approval body	IT Services
Ratified by	Nathan Indge
Publication	Supplied to new students at induction. Also published in the college virtual learning environment.

This policy and procedure is subject to The Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual orientation, Disability.

Transforming Lives Through Learning

Contents

Transforming Lives Through Learning

Overview

This policy relates to the organisation of Milton Keynes College which will be referred to as 'MKC' throughout this document. The term 'User' in the context of this document refers to any student or individual which has an account allocated for their use on the MKC network.

MKC recognises that users require use of computer hardware for accessing data, printing, Internet, messaging, and e-Mail services. However, we also recognise that these facilities carry with them some risks and liabilities.

It is therefore essential that MKC users accept and adhere to the guidelines in this document.

Security incidents resulting from non-acceptable use of MKC resources represent a significant cost to MKC, in terms of investigation time and remedial works to recover from them.

Scope

This policy applies to all users when using any MKC-owned desktop workstation, portable computer/tablet, or telephony device at all times.

It also applies when accessing MKC systems and resources from home or any remote locations, and when using user-owned devices on MKC wireless networks.

Purpose

- To assist users in the safe and responsible use of ICT and Internet based resources.
- To safeguard and protect the students and users within MKC, including their personal electronic data.
- To reduce to occurrence and impact of security incidents on the IT network, by clearly defining users' responsibilities in this matter.
- To protect MKC resources against theft or malicious damage.

Related MKC Policies

- Enrolment Form and Learning Agreement

Related Acts

- Computer Misuse Act (1990)
- Malicious Communications Act (2003)
- Communications Act (2003)

Policy Detail

Any breaches of this policy may result in disciplinary or legal action.

If students do not understand specific content within this policy, or are unsure of a course of action, they should seek clarification from their tutor in the first instance. If necessary, they will then consult with IT Services on the matter.

General Computer Usage

- MKC desktop/laptop computers, tablets, telephony devices, the Internet, and e-mail must be used primarily for study-related purposes.
- MKC reserve the right to monitor all aspects of its telephone and computer systems. MKC have the right to intercept or record any communications made by students, using telephone, Internet and e-mail.
- Computers, telephones, corporate Cloud based services (such as Office 365) and e-mail accounts are the property of MKC and are intended for study purposes. Therefore, users must have no expectation of privacy when using computers, tablets, telephones, e-mail or the Internet, whether it be for study or personal reasons.
- Users must not use MKC IT systems to access, or download material that can be considered/perceived to be obscene, extremist, defamatory or offensive to people who have protected characteristics in terms of equality. This includes material contained in jokes sent by e-mail. If users receive material with content of this nature, the material must be promptly disposed of. MKC reserves the right to use the content of user's e-mail in any relevant disciplinary processes.
- Any deliberate attempt to gain unauthorised access to facilities or system services via the MKC network is prohibited. This includes attempts to bypass accounting and logging systems. This also includes any attempts to bypass any web filtering products to access websites which are prohibited by this policy.
- Users of personal devices connecting to the MKC network either on-premises or remotely, are responsible for ensuring their devices are virus-free and have the latest security updates fully applied.
- Users must not transmit unsolicited commercial or advertising material via the MKC network.
- No MKC licensed software shall be copied to a removable storage device, or taken off site without the permission of someone from the IT Services team. The unauthorised or illegal copying of software may result in legal consequences and/or disciplinary procedures.
- No software or hardware shall be installed on MKC systems by any persons at any time without permission from IT Support department. This includes the running of the software from a removable storage device.
- Users must not deliberately waste staff efforts or networked resources, corrupt or damage another user's data, violate the privacy of others, disrupt the work of others, or otherwise use the MKC networks in a way that disrupts service to other users. All users must carry out housekeeping tasks to maintain their network storage and mailboxes within storage limits.
- Devices must not be left unattended and unlocked whilst logged into the network – this creates a possibility of unauthorised access to MKC systems. If being left unattended, the operating software must be locked and password protected to ensure this does not happen. User accounts are issued on an individual basis so that usage of the systems can be held accountable to a single user. Allowing others to use your network accounts is strictly prohibited. Any actions done under an account are accountable to the owner of that account, and may result in disciplinary procedures that are appropriate to those actions.
- Each user is responsible for the safeguarding of their system passwords. Default or temporary passwords must be changed at the earliest opportunity. For security reasons, individual passwords must never be printed, stored online or given to others. User password rights do not imply that the user has complete privacy. Use good practice when selecting passwords, and try to choose complex, 'hard-to-guess', or random passwords. Passwords must be at least ten characters in length.
- All data must be stored on appropriate network drives, or in approved Cloud storage. Any removable storage devices connected to MKC computers will automatically be encrypted with a minimum of 128-bit AES.

E-Mail Usage

- E-mail is a legal means of communication and therefore subject to the Malicious Communications Act 1988 and the Communications Act 2003.
- Users must not make derogatory remarks about employees, students, or any other persons. Any written derogatory remarks may constitute libel.
- E-mail must be drafted with care; it is a permanent form of written communication and can be recovered even when it has been deleted from your computer.
- To ensure e-mail communication is effective and efficient, users should not send trivial e-mails or copy-in other users unnecessarily.
- Users may use e-mail confirmation and receipt of important messages. This is not always possible and may depend on the system receiving the message. If in any doubt, confirm delivery/receipt of e-mail by an alternative method.
- Private use of e-mail is permitted, but must be confined to non-lesson time. The contents of personal e-mail must comply with the restrictions set in these guidelines.
- By sending an e-mail through MKC systems, the user explicitly consents to processing of any personal data contained in that message. If users do not agree with MKC processing such data, then another means of communication must be used.
- Subscriptions must not be made to any list servers or discussion groups that transmit material which does not comply with the objectives of MKC. This includes using a MKC e-mail address as a login name on third party sites for purposes that are not study related.
- The MKC e-mail system is intended for communication purposes, and not for data storage. Any e-mail attachment deemed important, should be moved to an appropriate network or approved Cloud storage location.
- Use of MKC e-mail is monitored and a copy of all e-mails sent is retained by the organisation for future audit and investigatory purposes.
- E-mail must be considered an unsecured medium when transmitting data. Sensitive and personal data must be transmitted by other means, or additional encryption tools should be used.

Internet Usage

- Limited private use of the Internet is permitted, but must not interfere with study, and must be confined to the user's own time. MKC actively monitors Internet use for content. If any material is viewed in error that does not meet the guidelines set out in this policy, a member of teaching staff must be informed.
- Under no circumstances should users view, upload or download any material that is likely to be unsuitable or offensive to other users at MKC. This applies to any content of a violent, dangerous, sexual or racist nature.
- Copyright applies to all text, pictures, video, and sound, including those received by e-mail or the Internet. Music and video files which are not free to distribute must not be downloaded or stored on any part of the MKC network.
- All Internet usage at MKC is constantly monitored, via random system checks and authorised investigations. This includes keywords which are submitted to search engines. All visited web sites are clearly logged as well as times they were accessed. Monitoring also applies to Internet usage on MKC devices being used remotely and on the internal wireless networks.
- The Internet must be considered an unsecured medium when transmitting data. Any transactions that originate from MKC are carried out entirely at the user's risk. MKC is not responsible for any on-line fraud that may occur from personal use, or the loss, damage or misuse of data.

Cloud Usage

- Personal and sensitive data should not be stored on any Cloud based storage, as this may be synchronised to local devices.
- The approved Cloud storage service provided to MKC users is Microsoft Office 365 OneDrive. This gives users the functionality to share files with others (including third parties). Users are responsible for ensuring that only appropriate information is accessed by others. MKC also provides a virtual learning environment for submission of coursework and sharing of study resources.
- Where local synchronisation is used with Cloud storage, users are responsible in ensuring that any locally stored data is synchronised successfully to the Cloud.