College Policy and Procedure for e-Mail and Internet Use

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 staff as a supplement to Conditions of Service. Also published on Staff Intranet.

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

Overview 3

Scope 3

Purpose 3

Related MKC Policies 3

Related Acts 3

Policy Detail 4

General Computer Usage 4

E-Mail Usage 5

Internet Usage 6

Cloud Usage 6

Social Networking 7

Data Protection 8

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 member of staff or individual from another organisation which has an account allocated for their use on the MKC network. Users will consist of direct employees of MKC and its partners as well as supply/contract staff.

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. Misuse of computers is covered by many UK laws which, as a responsible employer, MKC must advise its users of, to ensure they abide by these laws.

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. In addition, there may be direct financial impact, and indirect impact arising from damage to the organisation's reputation.

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

- Conditions of Service
- Professional Standards
- Safeguarding Policies
- Data Protection Policy
- Information Security Policy

Related Acts

- Computer misuse Act (1990)
- Data Protection Act (1998)
- General Data Protection Regulation (EU 2016/679)
- Malicious Communications Act (2003)

- Communications Act (2003)

Policy Detail

Any breaches of this policy will result in disciplinary action in line with the MKC Policy and Procedures for Staff Discipline. All cases of IT systems misuse will be treated as misconduct, and some serious cases may be treated as gross misconduct.

If employees do not understand specific content within this policy, or are unsure of a course of action, they should seek clarification from their line manager 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 work-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 employees, 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 work purposes. Therefore, users must have no expectation of privacy when using computers, tablets, telephones, e-mail or the Internet, whether it be for business 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 unless this is part of an authorised MKC campaign.
- 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. Software owned by MKC must not be copied without specific instruction and must only be copied when appropriately licensed, or for backup purposes. 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 safe-guarding 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.
- If a user has the ability to connect to other computer systems through the network, it does not give them the right make use of those systems, unless authorised to do so. Files belonging to other users must not be altered or copied, unless permission has been obtained by the owner of the file.
- All data must be stored on appropriate network drives, or in approved Cloud storage, so that it is secure and backed up. Storing personal data on local machines, particularly laptops, is prohibited. Personal data relating to staff or students must not be stored on any removable media whatsoever (e.g. CD/DVDs, USB flash drives, mobile telephones) to remove any risk of this information entering into the public domain via such devices. Any removable storage devices connected to MKC computers will automatically be encrypted with a minimum of 128-bit AES.
- Any release of personal staff or student data must be authorised by the appropriate Data Protection Officer. The Data Protection Officer must be consulted on all issues regarding the release of personal data.

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, competitors 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.
- E-mail signatures will automatically be configured as per the MKC branding guidelines.
- 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 not interfere with work, and must be confined to the employee’s own 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 business 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 by MKC staff 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.
- E-mail must not be automatically forwarded to third party accounts outside of MKC (e.g. Google, Yahoo etc.) E-mails often contain personal or sensitive information which should not be stored on a third-party system.

Internet Usage

- Limited private use of the Internet is permitted, but must not interfere with work, and must be confined to the employee's own time. MKC actively monitors Internet use for content, and the amount it is used by individuals. If any material is viewed in error that does not meet the guidelines set out in this policy, a member of the IT Services team 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.
- Users must not set up any web-site or social networking site which has references to MKC, or which is intended for use by MKC staff or students, without prior permission. References may include links, citations or images referring to MKC from a user's personal web space. Permission for such sites must come from the IT Services team, who will seek approval from the appropriate Senior Leadership Team.
- Any personal or social networking website of an individual MKC user in the public domain is expected to be conducted in a professional manner.

Cloud Usage

- Whilst it is accepted that staff and students may use personal Cloud storage (such as Google Drive, Dropbox etc.) for their own storage of files, and collaboration with third parties which may require use of specific products, no MKC data should be stored within these systems whatsoever. This includes any information or files produced by staff in relation to their role at MKC. Any data accessed on users' own Cloud storage whilst on MKC premises, or via MKC-owned devices must be in line with the requirements of this policy.
- Personal and sensitive data should not be stored on any Cloud based storage, as this may be synchronised to local devices. These should remain on traditional network shares or within management information systems.

- If exceptions are required which may breach these policy guidelines (e.g. when exchanging information with 3rd parties) then advice should be sought from the IT Services team to ensure appropriate levels of encryption are applied.
- 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. If extensive sharing of information is required, users should consider whether other methods are more appropriate such as Microsoft Office 365 SharePoint or shared network drives.
- Where local synchronisation is used with Cloud storage, users are responsible in ensuring that any locally stored data is synchronised successfully to the Cloud.

Social Networking

The following advice and guidelines are offered in a positive, supportive spirit and staff are advised to read and consider them carefully. The use of social networking sites such as Facebook, Instagram, LinkedIn and Twitter raise new challenges for professional staff working with young people and vulnerable adults in education.

Social networking sites encourage individuals to post personal and sometimes intimate information which previously would have been considered private. Anyone posting information through this media, must accept that this information could become public knowledge. At this point, whilst the activity may have taken place outside of work, it is no longer reasonable to assume that it is personal and private and nothing to do with third parties such as employers and authorities. Children and young adults may be naive in viewing this information and may, should they see staff role models in a different light, act differently or inappropriately.

If activities are shown to have brought MKC into disrepute, a member of staff would be in breach of the MKC Professional Standards, and disciplinary action may be taken. Other activities or information could compromise staff professional relationships with students and colleagues.

To help prevent these issues and mitigate risk, we advise staff of the following guidelines when using social networking sites, both within and outside of the organisation:

- Staff must not interact with students via social networking sites. This includes adding a student as a 'friend'. Any electronic communication to students and colleagues must be via the staff member's e-mail address. Consider carefully interactions with past students as they may also have relationships with current students. Users should not interact with any past students on social media who are under 18 years old, or those that have left MKC within the last twelve months.
- Staff must not set up groups or social networking sites which represent MKC without permission.
- When registering on social networking sites for their own personal use, users must register a private e-mail account, rather than their MKC account.
- Users are strongly advised to consider their privacy settings on social networking sites. These can be changed from time to time by providers. Any individual's social networking sites in the public domain, rather than private to friends only, must be in line with the MKC Professional Standards.
- All users must be aware that social networking sites can be used for cyber-bullying. MKC have a duty of care to our staff and students, and will take appropriate action in accordance with our policies and procedures for the elimination of harassment and bullying should we be aware that this is occurring. In addition, it is the responsibility of all staff to take appropriate action in accordance with these policies.

Data Protection

- Users of MKC systems must adhere to the policies stated in the Data Protection Act 1994 & 1998.
- Personal and MKC data accessed on our systems may be tracked for usage. Allowing third parties access to this information without permission from MKC is strictly prohibited, and will be treated as gross misconduct.
- Details of Data Protection are covered within the MKC Data Protection Policy. Users are advised to familiarise themselves with the content of this policy.