MK College Group

Building Fairer Futures.

MKCG Acceptable Usage Policy - Student

Author:	Executive Head of IT
Version:	3.4
Effective Date:	December 2025
Date of next review:	December 2027
Equality Impact Assessment completed:	
Reviewed and recommended by:	Executive Head of IT
Approved by and date:	Policy Scrutiny Group 24/2/26
Ratified by and date:	
Publication:	College Website / SharePoint / Student 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.

Alternative Format
This policy is available in alternative formats, to request this, please email marketingcampaigns@mkcollege.ac.uk

Version Control

Version Number	Author	Approver	Date approved	Next review date
3.4	Executive Head of IT	Policy Scrutiny Group	24/2/26	December 2027

Change log

Version Number	Summary of changes
3.4	Clarification of misuse with examples. Cross reference to Social Media and eSafety policy.

Contents Page

Introduction

Milton Keynes College Group (MKCG) recognises that users require use of computer systems 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 MKCG users accept and adhere to the guidelines in this document. Misuse of computers is addressed by many UK laws, therefore MKCG must advise its users, to ensure they are compliant with them.

Security incidents resulting from non-acceptable use of MKCG resources may represent a significant cost to MKCG, in terms of investigation time, liability and remedial works. In addition, there may be direct financial impact, and indirect impact arising from damage to the organisation's reputation.

Definitions

This policy relates to the organisation of Milton Keynes College Group (MKCG). The term '**User**' in the context of this document refers to any student, or individual with a student account allocated for their use on the MKCG networks. This includes use of the education networks within prisons.

Key words in this document are defined as follows (adapted from the IETF RFC 2119):MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement. MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition.
SHOULD: This word, or the adjective "**RECOMMENDED**", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT: This phrase, or the phrase "**NOT RECOMMENDED**" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behaviour described with this label.
MAY: This word, or the adjective "**OPTIONAL**", mean that an item is truly optional.

All data (whether electronic or paper) must be confidentially and securely destroyed once the retention period is reached.

Scope

This policy applies to all users when using any MKCG owned devices at all times including desktops, laptops and virtual desktops. It also applies when accessing any MKCG systems and resources from any remote locations (including at home), and when using user-owned devices on MKCG BYOD wireless networks within the campus.

Purpose

• To assist users in the safe and responsible use of Digital Technology and Internet based resources.
• To reinforce safe & appropriate behaviour with respect to IT usage
• To safeguard and protect the students and users within MKCG, including their personal data.
• To reduce the occurrence and impact of Information Security incidents on the IT network, by clearly defining users' responsibilities in this matter.
• To be clear and transparent as to the monitoring on the network and the expectation of privacy.
• To protect MKCG resources against theft or malicious damage.

Related Acts

- Computer Misuse Act (1990)
- Data Protection Act (2018)
- General Data Protection Regulation (EU 2016/679)
- Malicious Communications Act (2003)
- Communications Act (2003)
- The Equality Act (2010)

Policy Detail

All cases of IT systems misuse conflicting with the guidance in this document will be treated as misconduct. This may result in disciplinary action in line with the MK College Code of Conduct. Examples of IT misuse, include but not limited to: -

- Sharing of MKCG accounts, passwords or ID Cards in any form.
- Accessing illegal or inappropriate content through MKCG systems including the sending of malicious communications.
- Removing MKCG IT equipment from the campus without prior written permission, or leaving this in an unsecure location.
- Attempts to gain unauthorised access to MKCG systems or disrupt the access of others.
- Copying or distributing college owned software or data.

General Computer Usage & Data Security

Any communication should be structured in a professional manner. Derogatory or libellous communications relating to the MKCG, Students, Staff or any other person or company are prohibited. This includes MKCG systems, and external systems such as social media. Use of social media is detailed within the Social Media and eSafety policy for students.

You are responsible for the safeguarding of any passwords that you have. Individual accounts issued must not be shared with others. These passwords should not be written, printed, stored on any device or shared with others.

Students are responsible for all actions done under their account. Workstations must be locked when leaving desks, and you must log out at the end of a class/session.

Use of peer-to-peer, download accelerating or torrent software is prohibited through MKCG networks. No material which is illegal or infringes copyright should be brought into, or used on, MKCG premises.

Students 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 with protected characteristics.

Upon completion of your study at the MKCG, you will be required to return all MKCG IT equipment. The Data on such equipment is property of the MKCG. Self-service laptops from 'lapsafes' must not be removed from the campuses. Longer term loan devices are available in the study centres.

Students have a responsibility to report any infringement of the Acceptable Use Policy or IT Security Incidents to an appropriate staff member.

Any deliberate attempt to gain unauthorised access to facilities or systems via the MKCG network is prohibited including attempts to bypass accounting, web filtering and logging systems. This also includes carrying out any vulnerability scans without prior authorisation from IT Services. Only BYOD wireless networks may be accessed by student owned devices.

E-Mail & Internet Usage

The MKCG email system is provided primarily for your studies. No MKCG account should be used to sign up to external websites that are not linked or associated with your studies. Sites requiring verification of MKCG e-mail for student-based discounts are permitted.

E-mail is a permanent form of written communication and can be recovered even when it has been deleted from your computer. E-mail is a legal means of communication and therefore subject to the Malicious Communications Act 1988 and the Communications Act 2003.

The Internet must be considered an unsecured medium when transmitting data. Any transactions that originate from MKCG are carried out entirely at the user's risk. MKCG is not responsible for any on-line fraud that may occur from personal use, or the loss, damage or misuse of data.

Reasonable private use of the MKCG Internet system is permitted, in line with the general guidance of this policy. This includes accessing the Internet via the MKCG BYOD wireless networks on student owned devices.

Modern browsers allow the syncing of bookmarks, history and passwords between systems. Should users use this feature to sync items such as bookmarks/history to their own personal accounts, they are responsible for ensuring that any websites this includes are in line with the requirements of this policy.

All Internet usage at MKCG is continually 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 MKCG devices being used remotely and on the internal wireless networks. Local safeguarding software provides MKCG with daily reports which highlight any potential safeguarding issues and prevent incidents or concerns. Any use of inappropriate web content by students may therefore be reported to a member of the Safeguarding Team.

Security

When on campus you must wear your College ID/Access card at all times. If this is lost or stolen, you must report it immediately to prevent the possibility of unauthorised access. This card is for your sole use and must not be shared with other students. When utilising self-service lockers on campus, you are responsible for returning any devices that you have taken out on loan.

Students are responsible for the security of their own devices whilst on campus. This includes any devices that have been loaned temporarily for student use. Self-service laptop lockers are available on campus for learners to charge/store their electronic devices.

To prevent the risk of theft of systems used outside the campus you must take reasonable steps to ensure the safety of the equipment by not leaving the items in an unrestricted area or unsecure location. This includes any equipment that you may have on short term loan.

All work must be stored on OneDrive rather than local storage. Should an application not directly support OneDrive use, any files on other storage should then be backed up to OneDrive at a convenient time.

Use of Artificial Intelligence and associated technology

MKCG recognise AI technologies as a use resource of information, and direct study aid to our learners. We do advise learners of potential risks to their data, and malpractice when completing assessed work.

Before using an AI technology for assessed work, you must familiarise yourself with the guidelines within that particular assignment or exam. Whilst the use of AI may be permitted, this may still need to be referenced or declared. If the use of AI is permitted, this

does not suggest that it is required to pass an assignment or achieve a particular grade. Any use of AI technology outside of the assignment guidelines, or that which is not declared or referenced correctly, may be escalated in line with the following policies: -

- Student Code of Conduct
- Academic Misconduct policy

Students are advised that any personal data of their own or peers that is entered into AI engine, may be used to train the large language model (LLM). Therefore, we advise students to never share any personal information, data or images to these. This includes any personal use of Microsoft Copilot. The use of Copilot within the MKCG tenant including the 13+ version of Copilot (when available), is guaranteed not to be used for training the LLM, so is safe to use.