IT Acceptable Use Policy - Students

Author: David Few, Head of IT, MIS & Exams

Equality Assessment: David Few **Date: 27/08/2024**

Version and Date		Actions/Notes
1.0	August 2024	Merged Social Media policy into this policy. Added clear acceptable use guide in Section 7.

Approved by SMT: **August 2024**

Approved by Corporation: **22.10.24**

Date of Next Review: **August 2025**

Related policies or procedures or parent policy if applicable:
Data Breach Policy
Data Protection Policy
Online Safety Policy
Information Security Policy

Groups/bodies consulted in the development of the policy:
General Data Protection Regulation (GDPR) 2018
Data Protection Act 2018
Freedom of Information Act 2000
Privacy and Electronic Communications Regulations (PECR) Computer Misuse Act 1990
Counter-Terrorism and Security Act 2015
Regulation of Investigatory Powers Act (RIPA) 2000

To be published on College Website: Yes

To be published on Student Hub: Yes

IT Acceptable Use Policy - Students

1. Purpose

The purpose of this policy is to ensure that the students of Macclesfield College use the College's information and IT equipment in an acceptable way. It also includes the use of Macclesfield College's communication and collaboration platforms (including internet, email, cloud platforms, audio/video conferencing, messaging and telephony) and mobile IT equipment.

The College IT network and IT equipment provided by Macclesfield College are to be used for legitimateeducational, research, community and work seeking purposes. All users of the computers, laptops and tablets have a responsibility to use the resources in a responsible, lawful and ethical manner.

2. Scope

This policy applies to all students of Macclesfield College.

3. Computer Access Control

Access to Macclesfield College's IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and password are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the College's IT systems.

Individuals must not:

- Allow anyone else to use their User ID/token and password on any College IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access the College IT systems.
- Leave their password unprotected (for example, writing it on a note stuck to their laptop or on their Student ID card).
- Perform any unauthorised changes to College IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation to interrogate the system or data.
- Connect any non-College authorised device to the College network or IT systems.
- Store College data on any non-authorised College equipment.
- Give or transfer College data or software to any person or organisation without the authority of the College.
- Introduce computer viruses, spyware, malware and ransomware on the College network.
- Post anonymous messages or send broadcast messages.

4. Internet and Email

Use of college internet and email is intended for legitimate educational, research, community and work seeking purposes. Personal use is permitted where such use does not affect the individual's learning progress, is not detrimental to Macclesfield College in any way, not in breach of any term and condition of enrolment and does not place the individual or College in breach of statutory or other legal obligations.

Macclesfield College has a duty of care under the Keeping Children Safe in Education and the Prevent Duty to ensure that students access appropriate materials and know how to maintain their safety and security on the Internet. In order to do this the College will set certain firewall and web filtering policies to protect students from inappropriate and unsuitable resources and materials.

Where students are required for their course to research potentially sensitive materials such as violence, terrorism and extremism the teacher will advise the students in advance which websites are appropriate.

The College provides students with an email account and uses email as one of a variety of methods to communicate with students. Students should use their college email account appropriately and forward any suspicious / SPAM emails to the IT Student Helpdesk to investigate.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Macclesfield College considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use of the internet or email to make personal gains or conduct a personal business.
- Use of the internet or email to gamble.
- Use of the internet to reveal fellow student, staff or College sensitive/confidential information in a personal online posting, upload or transmission.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Download copyrighted material such as music media (MP3) files, film, video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet.
- Connect Macclesfield College devices to the internet using non-standard connections.
- Use of the internet to access or hack into unauthorised areas.
- Using the internet and college network to mine cryptocurrency.
- Play games on the Internet, unless under the direction of a tutor in a taught session.
- Use the internet, email or any other communication platform to bully or harass any member of the College's learning community.

The College retains the right to block websites that are deemed to be inappropriate and unsuitable for educational use in line with the UK Safer Internet Centre's 'Appropriate filtering guide for education'.

5. Cloud Platforms

All students at Macclesfield College are encouraged to use Microsoft 365 and OneDrive cloud computing storage at home and in college to save/access their files and documents. This gives all students 100GB of free storage space to save their college assignments and course files in a safe and secure environment.

All students will have access to our itslearning platform where they can communicate with their tutors, access their online course resources and complete their assignments.

6. Computer Hardware

All individuals are accountable for their actions when using the College's IT equipment.

Students may access the College network from computers, laptops and tablets within the College, personal devices and remote locations.

Students will be allocated an appropriate amount of disk space within the network and must ensure that they maintain backup copies of critical work throughout the year. They should ensure that they do not store any inappropriate or unnecessary materials within their user areas.

Students will be given an initial print credit at the start of their course; however, the student will be required to pay for any additional printing. Support is available via the Learner Support Fund from Student Services.

Individuals must not:

- Break, move or alter computer hardware.
- Modify data network hardware (cabling, communications devices etc).
- Remove hardware from college sites.
- Introduce any new hardware onto the wired network.
- Eat and drink within computer equipped classrooms

Students may connect personal devices onto the MLZ-Guest wireless network provided that it does not distract from their studies.

7. Acceptable Use Guide for Students

The College has defined what it regards as acceptable/unacceptable use for students and this is shown in the tables below.

Student actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking					X

comments that contain or relate to:	• Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to college networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Serious or repeat offences will be reported to the police.					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in college policies:	Accessing inappropriate material/activities online in a college setting including pornography, gambling, drugs. (Informed by the college's filtering practices and AUPs)				X	
	Promotion of any kind of discrimination				X	
	Using College systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the College				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the College or brings the College into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	Students			
	Not allowed	Allowed	Allowed at certain times	Allowed for relevant courses
Online gaming				X
Online shopping/commerce			X	
File sharing	X			
Social media			X	
Messaging/chat			X	
Entertainment streaming e.g. Netflix, Disney+	X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok				X
Mobile phones may be brought to college			X	
Use of mobile phones for learning at college			X	
Use of mobile phones in social time at college			X	
Taking photos on non-College managed mobile phones/cameras			X	
Use of other personal devices, e.g. tablets, gaming devices			X	
Use of personal e-mail for college data, or on the college network/wi-fi			X	
Use of College e-mail for personal e-mails	X			
Cryptocurrency Mining	X			

8. Viruses

The IT Support department has implemented centralised, automated virus detection and software updates within the College. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by use of approved College anti-virus software and procedures.

Students must tell a member of staff or the Student IT Helpdesk if they suspect a virus, malware or spyware has been introduced to the computers/network.

9. Student use of Social Media

The College may monitor social media sites it has access to. The College will instruct relevant parties to remove unauthorised material if necessary. This includes defamatory material, material that breaches copyright and will violate the Data Protection Act 2018 legislation.

Social media includes but is not exclusive to: Facebook, Twitter, Blogs (Blogger, WordPress etc.), LinkedIn, YouTube, Instagram, Pinterest, Snapchat, TikTok, WeChat, MeWe, Tumblr, Reddit, Telegram.

Students must be made aware of the impact they could have by posting their opinions and views via social media. It must be understood by students that they are integral to the College community and must restrict their opinions and views accordingly to avoid harm or offence.

Therefore, disciplinary actions will be taken if a social media post:

- communicates any messages that could be viewed as harassment or bullying or makes any liable claims.
- communicates any messages that breaks the College Equality and Diversity Policy or Anti-Bullying and Harassment Policy.

10. Actions upon Leaving College

All Macclesfield College IT equipment and data, for example laptops and mobile devices (including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Macclesfield College before your course's end date. Original purchase value of any unreturned devices or equipment, as logged in the IT Asset Register will be invoiced to students through Finance.

11. Monitoring and Filtering

All data that is created and stored on Macclesfield College computers is the property of Macclesfield College and there is no official provision for individual data privacy, however wherever possible the College will avoid opening student personal emails and files.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Macclesfield College has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with the Computer Misuse Act 1990 and Data Protection Act 2018.

The College understands that our students have a right to a certain degree of privacy at college and we aim to strike a balance between our business interests and our students'

expectations of privacy. The monitoring process should be fair and reasonable.

Students found abusing the rules will be removed from the network immediately and will be subject to the College's formal disciplinary procedures.

12. Reporting Security Incidents

It is your responsibility to report suspected breaches of information security without delay to the IT Technicians in person, the IT Student Helpdesk: itstudenthelpdesk@macclesfield.ac.uk or the College's Data Protection Officer (DPO): dpo@macclesfield.ac.uk

All breaches of information security will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Macclesfield College's student disciplinary procedures. This may also result in restrictions being placed on your IT account. Serious infringements of this policy may result in dismissal from the College and possible referral to the police.

13. Review and Monitoring

The relevance, efficacy and effectiveness of this Student IT Acceptable Use Policy will be reviewed in line with the annual cycle of strategic management activities to facilitate continuous improvement. The results of the review process will be analysed and changes made to the policy where appropriate.

MACCLESFIELD COLLEGE STUDENT IT ACCEPTABLE USE POLICY

I agree to the terms of the Macclesfield College Student IT Acceptable Use Policy

FULL NAME (PRINTED): **DATE:**

SIGNED: