Learner IT Acceptable Use Policy

Middlesbrough College Group

Contents

Introduction....3
Purpose....3
Scope....3
Definitions of Unacceptable Use....4
Network Use and Security....4
Network Security....4
Network Usage....6
Systems and Software Security....7
E-mail, Internet and Social Media....7
E-mail Use....7
Internet Use....8
Social Media Use....8
Guidance in Respect to Online Extremist Material....9
Exposure to Extremist Material....9
Use of Personal and College-issued Mobile Devices....10
Bring Your Own Device....10
MC Click Loan Device Scheme....11
Storing and Sharing Data....12
Network Monitoring....12
Precautionary and Disciplinary Actions....13
Backups and IT Technical Support....13
Inventions, Patents and Copyrights....14

Introduction

IT systems are critical to Middlesbrough College Group's ability to operate, and the College is continuously striving to promote and expand the use of IT across its services. As such, the College issues, or facilitates access to, IT hardware, systems and software that allow students to fulfil their learning experience. In order to safeguard staff, students and systems, it is expected that users of these resources do so in an appropriate, lawful and ethical manner.

The Data Protection Act (2018) and Computer Misuse Act (1990) require that information systems be kept secure against unauthorised access or disclosure, and the College has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed 'PREVENT', to protect its users from exposure to extremist material. It is important, therefore, that the College has a clear and relevant Learner IT Information Acceptable Use Policy.

All users are expected to read and comply with this policy, ensuring that all IT use is consistent with the College ethos, other relevant College policies, relevant national and local guidance and the law.

Purpose

All users of College IT systems have a responsibility for safeguarding staff, learners and systems from malicious or negligent use. The purpose of this policy is to describe these responsibilities, and the manner in which they are to be implemented.

Successful implementation of this policy will ensure:

- all learners are aware of their responsibilities, and fully comply with the relevant legislation and policies;
- all learners are aware of how network monitoring will occur and the range of disciplinary actions to be used if the systems are used inappropriately;
- users are protected from inappropriate material and are aware of the reporting methods if such material is identified;
- information is stored, shared and accessed in a secure and consistent manner;
- authorised users can securely access information to perform their roles;
- all of the College's IT facilities, systems, data and equipment are adequately protected against intentional or unintentional abuse which may otherwise lead to a reduction or denial of service to all College users;
- the College meets its legal responsibility to ensure that all users of College IT systems work within the requirements of the relevant acts, regulations and laws; and
- prevention of any activity on the College IT networks that could bring the College into disrepute or cause financial or legal penalties.

Scope

This policy is applicable to all students who use, or connect to, Middlesbrough College Group IT systems and/or hardware.

IT hardware includes, but is not limited to, computer workstations, laptops, mobile phones and tablets, including 'bring your own devices' (BYODs) and 'MC Click' loan laptops.

IT systems include, but are not limited to, Wi-Fi, applications, email, file storage, management information systems (MIS), databases, telecommunications and cloud services.

This policy is designed to cover the use of all IT resources across all Middlesbrough College Group locations. New and developing technologies may not be explicitly referred to but should be considered to be included in the scope of this policy.

Definitions of Unacceptable Use

The following is an inexhaustive list of unacceptable uses of IT resources:

- viewing, creating or transmitting any material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence;
- viewing, creating or transmitting offensive, obscene, indecent or extremist material;
- viewing, creating or transmitting defamatory material;
- interfering with the work of others or the system itself;
- sending of any message internally or externally which is abusive, vulgar, humiliating, hostile, critical, embarrassing or intimidating;
- communicating and/or interacting inappropriately with staff or students via e-mails, the internet, mobile telephones or any other electronic means of contact;
- gaining unauthorised access to or violating the privacy of other people's files, corrupting or destroying other people's data or disrupting the work of other people;
- creating or transmitting material such that the copyright of another person is infringed;
- downloading any files unless virus scanned;
- gaining deliberate unauthorised access to facilities or services accessible via local or national networks;
- transmitting by any method, any confidential information of the College, otherwise than in the normal course of duties as identified by the College;
- disclosure of passwords to any other person or party;
- use of any non-encrypted media (CDs, DVDs, USB flash drives, etc.) to store or share any sensitive or College-owned data;
- purposely bypassing Middlesbrough College Group security systems, including via the use of VPN or other proxy tools.

Network Use and Security

Network Security

You must be a currently registered student with a designated ID to use the Middlesbrough College Group network. This ID and a temporary password will be issued at enrolment/induction.

Users must:

- change any temporary passwords upon first logging in;
- keep network passwords secure and log out of any workstation before leaving it unattended; and
- only log on, or use any machine, using your own password or credentials.

Users must not:

- introduce viruses or other disruptive elements to the system;
- use encrypted files (unless prior written permission is obtained from your tutor, and the keys or passwords made available to the IT technical support staff);
- circumvent Network Access Control; or
- copy, download, distribute or store any music, video, film or other material, for which you do not hold a valid licence or other valid permission from the copyright holder.

Passwords:

Users must create strong passwords that have the following characteristics:

- contain both upper- and lower-case characters;
- include a mixture of alphabetic, numeric and special characters e.g., 0-9, !@#$%^&*()_+|~-=\`{} []:";'<>?,./); and
- are at least eight characters long.

Passwords must not:

- include personal details which may be readily known to others, or can be easily found in a social media profile (e.g., partner's name, birthday, names of pets, etc.);
- include the user's User ID, or any variation thereof (e.g., reversing);
- use common sequences of numbers or letters (e.g., 12345678 or qwerty, etc.);
- include anything listed above modified by:
  - reversal: zzatsjl -> ljstazz;
  - appending or prepending a single character: Marylin1 or 9Charles;
  - substituting digit 0 for letter O or digit 1 for letter l: apri1f001;
  - appending to itself: johnjohn;
- be trivial, predictable or obvious; or
- be used for other College or non-College accounts, whether current or historic.

A good technique to create a strong password is to use a passphrase formed from a made-up statement that can be easily remembered. This should consist of letters, numbers and special characters which are used to represent the words or meaning of a phrase, for example:

My house is the 9th at Eastgate Terrace = MhIt9th@ET

Users are encouraged to use a password manager, which can create and store strong passwords that would otherwise be difficult to remember.

Passwords help to ensure that only authorised individuals access a computer system and can also help to establish accountability for all transactions and changes made to data or files within a system. Poor password protection may lead to a breach of systems and information. Users are accountable for all activity on their account, irrespective of who used the account or has the password. The Computer Misuse Act (1990) covers unauthorised access to computer systems, including the use of another person's identity. If a user allows access to their account and password to another individual who then breaches the Computer Misuse Act, both individuals could be deemed to have committed an offence.

Users must always keep their password secret by adopting the following protocol:

- Treat all passwords as sensitive and confidential information.

- Do not share the same password with anybody else.
- Do not divulge passwords to any unknown party, whether verbally, digitally or in written form (a user should never be asked to reveal their password by Digital Services or any other College department).
- Do not write passwords down.
- Lock devices when not in use or when left unattended.
- Do not make password hints obvious in content or format (e.g., “my family name”, “my birthdate.pet’s name”).
- Report all security incidents, including actual or potential unauthorised access to the College’s IT systems, immediately to the Help Desk.
- If an account or password is suspected to have been compromised, report the incident as soon as possible to the Help Desk. Immediately change all passwords which may have been compromised.
- Do not autosave passwords when using a public computer.

External access to all Middlesbrough College Group systems is subject to Multi-Factor Authentication (MFA). You will be prompted and guided through the process when you log onto the College system. The on-site Help Centre is available to address any problems by logging a ticket or calling 01642 33(3444).

Refer to MC70 IT Password Policy for further information regarding the use of passwords.

Network Usage

You may use the Middlesbrough College Group network and computing resources to create, view and transmit work relating to your College activities. Network access rights and saved files will be deleted when you leave the College, so you should not keep files on the network that you will need once you have left. You may not at any time create, intentionally view or transmit any images, literature or other data that:

- are offensive, obscene, indecent or defamatory;
- are designed or likely to cause annoyance, inconvenience or needless anxiety, e.g., bullying or harassment of students, staff or others by email or other means; or
- infringe the copyright of another person.

The College offers a monitored wireless service (Wi-Fi) for users. Connection to the College wireless network (eduroam) requires a valid username and password (the same details you use to log in to any College computer). By using the College wireless network, all users agree to adhere to the Acceptable Use Policy.

Users must not attempt to breach the security or filtering measures of the College network and must not download illegal software via this network. If downloading content from the internet, it is the responsibility of the user to ensure that they adhere to the requirements of the publisher, as well as copyright laws.

Users must not physically connect any personally owned device to the College network without prior agreement with the Help Centre.

File storage:

The college will provide all students with a OneDrive (Office365) storage which can be used to store college files. The user is responsible for the content and maintenance of their

network drive. OneDrive repositories should not be synced with non-Middlesbrough College devices in accordance with Data Loss Prevention guidelines.

You should ensure that you save all of your files to your OneDrive folder and not to your desktop. There is a risk of losing your data if saved to desktop, as these files are not backed up and cannot be recovered.

Files older than one year on Collee systems will be subject to automatic archive.

Systems and Software Security

To ensure the security and integrity of College systems, you must only use applications pre-installed on any Middlesbrough College Group network, on any Middlesbrough College Group device or on Middlesbrough College Group supplied media.

Office 365 should be used to share data with students, Middlesbrough College Group staff or external parties in relation to your work. This is the recommended process for sharing data although e-mail may also be used. Be aware that the College antivirus system may automatically delete infected files.

Unless you have specific consent from a tutor or from your tutor, you must not:

- interfere with the software or hardware configuration of networked equipment or systems in any way;
- install, download or use any additional software on college devices, this includes free and open-source software;
- install, download or use any copyrighted material (such as pictures, films, music or word files), without written consent from the copyright holder or an acknowledgement of the original source of the material, as appropriate;
- connect personal laptops or other mobile devices to the network, other than through the eduroam wireless system; or
- use VPNs or proxies on any device connected to the Middlesbrough College Group network.

E-mail, Internet and Social Media

E-mail Use

The College arranges for every student to have an email account which is administered for the College by Microsoft (Office365), including setting filters for viruses and spam mail, etc.

When you send messages outside the College your mail address identifies the College as being the mail account provider. You have a responsibility to ensure that the communications that you send do not involve the College in any potentially embarrassing or libellous situations.

Students should be aware that the College may access or remove these accounts at any time. Misuse of e-mail messages sent from or to these e-mail accounts can inform or be the basis of College disciplinary actions.

College e-mail accounts will remain live for one month after the end of your course, after which they will be deleted along with all data in associated cloud storage.

Bulk Email

'Bulk Email' refers to the use of email to send messages to large groups of recipients, either by using large distribution lists or by manually selecting many recipients.

Bulk email must only be sent by authorised users to send important communications, which are relevant to all or most recipients, and you must have permission from your tutor before sending. Regular use of bulk email is to be avoided.

Internet Use

The internet is a valuable tool for your college work. Reasonable private research on the internet is allowed if it does not interfere with your college work, however you must not:

- take up a workstation which is required by other students for their work (e.g., at peak times in the LRC); or
- play online games or use gambling sites.

All users of the network have their internet use automatically monitored and a record of sites visited is recorded by IT technical support.

Social Media Use

A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chatrooms, media posting sites, blogs and any other social space online. Social media includes, but is not limited to, sites such as Facebook, Twitter, TikTok, Snapchat and Instagram.

This policy applies to the use of social media, whether during College opening hours or otherwise. The policy applies regardless of whether the social media is accessed using Middlesbrough College Group IT facilities and equipment or via personal facilities and equipment.

Your interactions on social media should be polite, and you should actively respect the environment in which we all work. You are ambassadors for the College and are responsible for how your behaviour and language impacts on the good reputation of the College. Be aware that information posted on social media may be permanently available and always consider future implications before posting. These expectations apply both on- and off-site and on- and off-line, including comments you post about Middlesbrough College Group via social media.

You must:

- immediately report any post, comment or discussion that disparages or brings the College into ill-repute.

You must not:

- engage in activities involving social media which might bring Middlesbrough College Group into disrepute;
- represent your personal views as those of Middlesbrough College Group on any social medium;

- discuss personal information about students or staff at Middlesbrough College Group; or
- use social media and the internet in any way to attack, insult, abuse or defame students, their family members, staff, other professionals, other organisations or Middlesbrough College Group.

You may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

The College recognises that students may desire to use social media for personal activities by means of College computers, networks and other IT resources and communications systems. The College authorises such use so long as it does not involve unprofessional or inappropriate content and does not interfere with learning responsibilities or productivity. Excessive use of social media that interrupts authorised user's productivity may invoke disciplinary procedures.

Guidance in Respect to Online Extremist Material

The risk of global online radicalisation is considerable and has resulted in vulnerable young people and adults travelling to conflict zones to support terrorist groups or committing lone operative attacks within the UK.

Reducing the presence of extremist groups online is the responsibility of all College users. All extremist groups have a significant online presence which makes access to such material relatively easy. Such groups use many platforms including websites, chat forums, YouTube and Dailymotion, along with social media platforms including Facebook, Snapchat and Twitter. Middlesbrough College Group, in conjunction with Cleveland Police and Middlesbrough Council, have a set protocol in relation to reporting extremist material online.

Exposure to Extremist Material

Middlesbrough College Group permits learners to make use of computers as part of learning. Our filtering systems are designed to prevent access to known extremist material, but individuals can be ingenious and resourceful, devising ways to bypass security systems. On occasion web filtering may not successfully block all extremist material, particularly as publisher's endeavour to circumvent detection systems.

If you observe potentially extremist material online, please follow the procedure below:

1. Take a screenshot of the page using the Print Screen button on your keyboard.
2. In Outlook, start a New Email. In the main body of the email type a short description (e.g., "I was on eBay and this link popped up, so I have referred this to you"). Right click and paste the screenshot image into the email.
3. Enter "Extremist Material Online" into the Subject field, then send the email to safeguarding-team@mbro.ac.uk.

4. If a social media issue (Facebook, Instagram, Twitter etc), report the page or post using the platform's reporting facility.

If you observe a fellow learner with potentially extremist material open on the screen, please follow the procedure below:

1. Take a note of the computer location, the date and time of the incident, and the name of the learner if possible.
2. Send an email report to safeguarding-team@mbro.ac.uk as follows:

   Subject: PREVENT

   Report Body Text:

   - computer location;
   - date and time of the incident;
   - details of the learner;
   - description of what you observed.

The safeguarding team will then ensure that the incident is investigated and escalated as appropriate. If you feel concerned or worried by any material you may have witnessed, please contact the safeguarding team immediately.

Use of Personal and College-issued Mobile Devices

Bring Your Own Device

The College seeks to promote the effective and safe use of information systems to ensure a productive environment for learning and teaching. 'Bring your own device' (BYOD) means accessing College systems and information through personally owned devices such as tablets, smartphones and laptops. The College recognises the benefits of a flexible BYOD approach; however, BYOD must be carefully managed to ensure that standards of information security are not compromised.

The College is responsible for the data which it holds and manages that data in accordance with the Acceptable Use Policy, the Data Protection Policy, and the Data Protection Act 2018.

The Data Protection Act clearly sets out the responsibilities for those storing and handling information. The College is fully committed to ensuring that the principles of the Acceptable Use Policy and Data Protection Act are adhered to, regardless of whether the user is accessing data on a College-owned or personally owned device.

Any College data stored on a personal device is owned by the College. Users must not save any College-owned data which may be considered personal, sensitive, confidential or of commercial value to personally owned devices. The College reserves the right to clear data stored on any personally owned device which has been used to access College data. This may also result in the removal of any personal data stored on the device.

Digital devices are not permitted for use in changing rooms, locker rooms, toilets or bathrooms.

The College provides information systems such as College email, website, VLE, Apps Anywhere, etc., which allow secure access to data using an internet browser. When using personal devices to access College systems, users should:

- adhere to any classroom or tutor rules in relation to digital devices;
- clearly separate personal usage and College usage on any BYOD device;
- disable automated, cloud hosted, back-up services on any device which is used to access College data;
- ensure the device is correctly secured with relevant security software and is protected by biometrics and/or pin/security code;
- ensure the device has auto-lock enabled (device locks automatically after an idle time period);
- ensure the device is not cached to remember passwords;
- ensure that they log out of any College sites after use;
- set up remote wipe capabilities, which ensure that the device can be 'wiped' of all data in the case of loss or theft; and
- securely remove all College data when their relationship with the College ends.

Communications with other students and members of College staff must always be respectful and appropriate, regardless of whether this is in-person or digitally. Messaging and communications platforms such as WhatsApp, AirDrop, Bluetooth, Facebook Messenger and Instagram must not be used to distribute inappropriate or offensive messages or media.

Middlesbrough College Group reserves the right to monitor any on-line communications for improper use. Electronic communication and/or downloaded material, including files deleted from a user's account, may be monitored, or read by Middlesbrough College Group officials.

The College takes no responsibility for the maintenance, support or costs associated with personally owned devices.

MC Click Loan Device Scheme

Those students in receipt of a laptop as part of the MC Click Scheme must in addition acknowledge and comply with the following:

- Learners in receipt of a loaned digital device are solely responsible for its care and proper use at all times.
- Loan digital devices should be brought to college fully charged and taken to every session unless advised otherwise.
- Learners will not use loaned digital devices to access and/or view internet sites or materials that are otherwise blocked or prohibited.
- Learners with loan devices should keep all account and personal details, including home addresses, and telephone numbers, private.
- The loaned device shall mainly be used in College for its primary purpose: online and digital education and learning.
- Inappropriate device use may result in the removal of the loan device and enactment of the Middlesbrough College Group Disciplinary Procedure.
- Learners who use mobile or digital devices to disrupt lessons may be subject to disciplinary action and removal of the device.

- The device must be returned to Middlesbrough College Group on completion of the course of study or any other defined reason in line with the terms and conditions of the scheme.
- Loan devices may be remotely locked and blocked by Middlesbrough College Group.
- The reasonable use of MC Click loan devices for personal usage is allowed, however all data will be wiped from the device when it is returned to the College. The learner must not perform any activity which contravenes any of the rules listed in this policy.

Middlesbrough College Group reserves the right to manage and secure MC Click devices with any required software for the duration of the student's studies with Middlesbrough College Group.

Storing and Sharing Data

File and data sharing is an essential aspect of many College courses. College data must be securely handled to ensure its security and integrity.

Users must not transfer any College-owned data which may be considered personal, sensitive, confidential or of commercial value to personally owned devices.

The preferred method of file storage and sharing is via cloud storage in SharePoint or OneDrive, allowing the user to access the file from any internet-enabled device. This method of sharing ensures that the document remains 'owned' by the sender and access can be revoked or amended at any time if required. Data stored within these services is held by a third party. However, ownership of the College data remains with the College and responsibility for the security of that data remains with the user. Storage quotas are applied to all network accounts. You are advised to remove all large and unwanted files as soon as possible after using them so that you do not take up unnecessary space on the system.

Data may also be shared by the use of an encrypted USB drive. Any College data transferred via a USB drive should be securely deleted from the USB drive once the transfer is complete.

Any suspected data breach must be immediately reported. Further information regarding information security can be found in MC64 IT Information Security Policy.

Network Monitoring

The contents of College IT resources and communications systems are the property of the College. Therefore, authorised users should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on College electronic information and communications systems.

The College reserves the right to monitor, intercept and review, without further notice, authorised users' activities when using College IT resources and communications systems, including but not limited to social media postings and activities, to seek to ensure that our rules are being complied with and for legitimate business purposes. Authorised users consent to such monitoring by their use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting,

reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

The College may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

When logging on to the College network you confirm that you accept the IT Acceptable Use Policy. In accepting this policy, you are consenting to all clauses within it. For clarity, the following information is routinely logged for monitoring purposes:

- dates and times of logins and logouts;
- applications and data accessed;
- e-mail metadata including sender, recipient, subject, date and time;
- web pages accessed with times and dates; and
- antispam and antivirus events.

In addition, the College wishes to make you aware that Close Circuit Television (CCTV) is in operation in the College for the protection of employees and students.

Any Middlesbrough College Group staff member may ask a student to explain their activities on a computer at any time, if they believe that the use may be inappropriate according to this policy and guidelines.

Precautionary and Disciplinary Actions

Attempted access to blocked or inappropriate websites is logged and instant alerts are triggered to appropriate personnel across the site. Inappropriate browsing may result in an audit of a user's internet browsing history and may be subject to disciplinary proceedings. It is acknowledged that access to sites or material that the College has agreed be filtered may be necessary for research or other academic teaching purposes. An exemption may be applied for via the IT Manager.

For the protection of the integrity of the network:

- IT technical staff can at any time temporarily remove a user's access to the network if any unacceptable use has been made or is suspected.
- Misuse will be dealt with under the college disciplinary system. Appropriate actions will be taken according to the level of misuse.
- In some cases, the College may be legally obliged to contact the police or other authority if the incident warrants it.

In addition, the Middlesbrough College Group network is part of a larger network community called JANET. The College is responsible for users' conduct on this network and will implement disciplinary action if our standing as a member is compromised.

Backups and IT Technical Support

Although security of the network is maintained and backups of your network files and folders are taken regularly, it is your responsibility to ensure that you have your own backups of critical work in case of loss of your files due to accidental erasure.

Files stored on your desktop are not backed up and therefore cannot be recovered in the event of device failure.

The Help Centre staff are there to assist you. If you require further information or help about the use or set up of your computer, or have worries about the security of your work, you should contact the Help Centre, either in person, by logging a ticket or by calling 01642 33(3444).

College equipment can only be maintained to a high standard with the help of all users. Students must report faulty equipment, and must not tamper with, remove, transfer or relocate equipment without authorisation from a tutor.

Inventions, Patents and Copyrights

Users are required to inform the College immediately of any invention, improvement, discovery, process, design or copyright which they create or obtain whilst in the College's employment or as a consequence of it. This will become the absolute property of the College except as otherwise stated by statute. Users irrevocably waive all moral rights under the Copyright, Designs and Patents Act 1988 in any existing or future works created by them.