

E-Safety Policy

Document Control	
Document Type	Policy
Date Approved	October 2021
Approved by	Principalship
Review Date	August 2022
Department	Student Support and Experience
Policy Owner	Assistant Principal Foundation Studies and Student Support
Principalship Lead	Vice Principal Student Experience and Support
Accessible to Students	Yes

SCOPE AND PURPOSE

This policy covers:

- Anyone logging into any network, service, website or portal associated with the College/UCEN Manchester
- Connecting a device via the College/UCEN Manchester network
- Any electronic communication with a College/UCEN Manchester Student, member of Staff or contractor
- From any geographic location both on Campus and off Campus.

POLICY VALIDITY

This policy is valid for the academic year 2020/ 21 and is due for review in summer 2021.

RESPONSIBILITY

The reporting responsibilities for e-safety follow the same lines of responsibility as the College/UCEN Manchester Safeguarding Policy.

All Staff

- Are responsible for ensuring the safety of students
- MUST report any concerns or disclosures immediately to a Designated Safeguarding Person (DSP) and recorded on My Concern
- Should NEVER offer assurance of confidentiality; everything discussed MUST be reported
- MUST keep to the terms and conditions of the IT Acceptable Use Policy at all times
- MUST attend staff training on safeguarding and e-safety and display a model example to students at all times
- MUST actively promote safeguarding through embedded good e-safety practice.
- MUST communicate with students professionally at all times.

Students:

- MUST keep to the terms and conditions of the IT Acceptable Use Policy at all times
- Receive appropriate e-safety guidance as part of their programme of study
- Inform a member of staff when they are worried or concerned an e-safety incident has taken place involving them or another member of the college /HE community.
- MUST act safely and responsibly at all times when using the internet and/or mobile technologies.

Monitoring

The Manchester College/UCEN Manchester monitors, logs and reports on students and staff use of IT systems and IT network usage as part of the College's/UCEN Manchester's responsibility towards the 'safeguarding of young people and vulnerable adults' and Prevent duty for terrorist and extremist behaviour.

Any attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the College's/UCEN Manchester's disciplinary process.

Where requested this information will be securely shared with appropriate local authorities and external support agencies.

Head of Student Support - Safeguarding Lead

The student experience and support department is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out in collaboration with Curriculum and IT support services *by* receiving regular information about e-Safety incidents and monitoring reports to include:

- On the agenda for the Safeguarding Strategy Group
- Regular monitoring of e-Safety incident logs - via Impero reporting and feedback at department meeting agendas from Heads of Department Student Support (HoDs SS)
- HoDs SS have a duty of care for ensuring the safety (including e-Safety) of students, though the day to day responsibility for safety.
- HoDs SS being aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.
- The HoD SS safeguarding lead is responsible for ensuring that the designated safeguarding practitioners and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The AP and HoDs SS will ensure that there is a system in place to allow for monitoring and support of those in College/UCEN Manchester who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

HoDs Student Support:

- takes day to day responsibility for e-Safety issues
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides (or identifies sources of) training and advice for staff
- liaises with (College/UCEN Manchester's) technical staff
- receives reports of online safety incidents from Impero and creates a log of incidents on My Concern to inform future online safety developments.
- meets regularly with HoD SS - Safeguarding lead and AP, to discuss current issues, review incident logs and if possible, filtering / change control logs through a standardisation approach in collaboration with director of IT
- attends relevant meeting reports regularly to College Leadership Team where appropriate

Director of IT / Technical staff:

- The College/UCEN Manchester has a managed ICT service provided by LTE Group Operations. The LTE Group IT Services team will work with the College/UCEN Manchester to ensure all online safety measures are implemented in collaboration with the college safeguarding team, ensuring the College's/UCEN Manchester's IT infrastructure is secure and meets best practice recommendations

- Filtering and monitoring is undertaken by multiple systems that overlap to provide comprehensive protection and auditing capabilities.
- There will be regular reviews and audits of the safety and security of College/UCEN Manchester technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Where appropriate users will be provided with a username and secure password, users are responsible for the security of their username and password
- Information Services are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- **Bring Your Own Device (BYOD)** BYOD is permitted and encouraged in College/UCEN Manchester. All students have appropriate access to systems they require using their own device both on the College/UCEN Manchester WIFI and over the internet.

Quality Team

Group Quality Manager (Digital Lead) will develop and implement the Digital Learning strategy for The Manchester College (TMC) & UCEN Manchester.

The aim of the strategy:

- Enhance teaching, learning and assessment through the use of digital technologies
- Embed digital learning across all business areas to achieve a blended curriculum offer
- Develop the digital capabilities of teachers and students
- Improve access to digital learning for all students
- Create a culture of digital innovation alongside the assurance of safety first.

Safeguarding Strategy Group

The Safeguarding Strategy Group provides a consultative group that has wide representation from the LTE Group community, with responsibility for issues regarding online and monitoring the online policy including the impact of initiatives.

Members of the Safeguarding Strategy Group will assist the with:

- the production / review / monitoring of the online policy / documents.
- reviewing the online curricular provision along sided the Quality team
- monitoring network / internet / incident logs where possible

Parents, Guardians and Next of Kin:

For students under the age of 18, the College recognises the important role that parents, guardians and next of kin play in supporting their young person to stay safe online.

College will take every opportunity to help parents understand these issues through *parents' events, newsletters, letters, parent portal and the website.*

Covid addition:

During the Covid-19 pandemic, the introduction of remote and blended learning and an increase in the use of online learning has required a refreshed approach to online and e-safety with the introduction of a code of conduct for online lessons and a new Digital Learning Strategy, which has been led by the Quality team.

To support students to engage with their Study Programme remotely, we have agreed to **loan** any learner who needs support accessing learning at TMC/UCEN Manchester with a laptop or iPad. The laptop/iPad loan is to support directly with activity associated with the students' Study Programme. Continuation of this loan arrangement is dependent upon continued attendance on the Study Programme and full engagement in activities as directed by Curriculum and/or Support Services. All students must have signed the equipment scheme agreement and understood this policy.

Do's and Don't

The points below offer guidance on appropriate use of online communication. Any breach of this guidance may be referred to the College/UCEN Manchester disciplinary procedure.

Any breach considered to be a criminal offence will be referred to the police for investigation.

The appropriate use of communication applies to all devices and services, which might include:

- Computers, Laptops & Mobile devices (including phones and tablets)
 - Game Consoles
 - Email, Instant / Direct Messages & Chat rooms
 - Social Media
1. You must not create, store, exchange, display, print or circulate any message or media which may cause offence to others.
 2. You must not post or circulate any message which may be considered harassment.
 3. You must not send messages at random or excessively, also referred to as "spamming".
 4. Staff must not use personal devices or accounts as a method of communicating with students.
 5. Staff must not give personal contact details to students.
 6. Student contact details must never be stored on a staff members' personal device(s), including computers, laptops, mobile phones, tablets, personal cloud or personal storage devices.
 7. Staff and students must not make or receive personal calls, messages or emails etc. whilst in a teaching environment.
 8. College/UCEN Manchester devices may, on occasion, be used to gather either video or photographic evidence in order to support students' course requirements provided that the College/UCEN Manchester hold a signed authorisation form for the student in question. All personal images will be held in accordance with GDPR guidelines.
 9. You must not give out any personal information such as contact details, financial information or passwords (however this is not an exhaustive list).
 10. You should not open files or emails from people you do not know. They may contain viruses or offensive material.

11. If you see something abusive or upsetting online, you must report it to a designated safeguarding person.
12. You should not save your log-on details on shared computers as some people may use your screen name to defraud or scam people in your contact lists.
13. There may be legal implications if the Internet is used for criminal intentions for example to intimidate or to extract financial information for personal gain. All conversations using College/UCEN Manchester IT systems are captured and recorded on the College's servers.
14. You must not post any confidential information to any online platform.

If your post could be considered as representing or being associated to the College/UCEN Manchester in any way, then:

- It is imperative to portray a balanced tone when raising politically sensitive issues.
- When linking to websites not controlled by the College/UCEN Manchester (such as to relevant news articles) it must be clear that the link is external. No communication should be made with students from personally created user accounts or phone numbers. Only approved online messaging services can be used to communicate with students, all communication must be via a College/UCEN Manchester user account these include:
 - Email (using a College/UCEN Manchester account)
 - Microsoft Teams and Microsoft Office 365 collaboration (using a College/UCEN Manchester account)
 - SMS (using a College/UCEN Manchester device).

Training

Students:

How to guides will be available via the website and through the Student Hub intranet. Tutorial planning will include appropriate and relevant safety sessions for students and enrichment staying safe themes will include the associated risks online, for instance in relation to PREVENT and radicalisation and in Relationship and Sex Education enrichment and awareness raising campaigns throughout the year.

Issues associated with E-safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and mobile technologies.

Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. Induction sessions and the Report for Support links on the Student Hub will support this process.

Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

For staff:

Staff will receive training on the Digital Strategy and code of conduct, alongside new technology developments through regular CPD hosted by the Quality Team. Updates to safeguarding training take part annually against a detailed training matrix, which links to the KCSiE (Keeping Children Safe in Education statutory guidance) with mandatory sessions logged within HR.

Social Media

Use of The Manchester College and UCEN Manchester social media accounts

Only employees who have been authorised to use social media accounts through the LTE Group's Communications team may access social media on the College/UCEN Manchester network or create, maintain, or post on behalf of official College Group accounts.

The use of social media will only be approved where it is deemed to benefit students and learning, is in the business interests of the College, and meets EDI, safeguarding and PREVENT duties.

The College/UCEN Manchester has a number of official social media communications channels, which are part of the College/UCEN Manchester infrastructure. These take priority in externally published documents and materials.

In the event of an incident or emergency involving the College/UCEN Manchester no content should be posted to any social media channels except by the Marketing and Communications team who will manage PR centrally.

New social media accounts that use an official logo or College/UCEN Manchester name must not be created unless approved through the Marketing and Communications department. All social media accounts must be accessible by a second administrator at all times, preferably a line manager.

When an administrator leaves the College/UCEN Manchester, their access to College/UCEN Manchester social media accounts must be revoked, and the account either handed over to another administrator or closed.

Online privacy and personal information

College/UCEN Manchester employees must be aware of their social media presence, particularly when the social media account openly states that they work within the College/UCEN Manchester.

Your social media presence on sites such as Facebook can contain a lot of personal information that you might not wish to share with your colleagues, employer or the general public.

Unless your privacy settings are restricted, your colleagues, employers and students may be able to access your personal information. Therefore, it is important to ensure that your privacy settings reflect the amount of information you want people to find out about you.

Cyber Bullying

Cyber bullying is a form of bullying. As it takes place online, it is not confined to College/UCEN Manchester buildings or College/UCEN Manchester hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable.

Cyber bullying includes bullying via:

- **Text message and messaging apps** e.g. sending unwelcome texts or messages that are threatening or cause discomfort.

- **Picture/video-clips** e.g. using mobile device cameras to bully someone, with images usually sent to other people or websites.
- **Phone call** e.g. silent calls or abusive messages. The bully often disguises their number.
- **Email** e.g. emailing upsetting messages, often using a different name for anonymity or using someone else's name to pin the blame on them.
- **Chat room** e.g. sending upsetting responses to people when they are in a web-based chat room.
- **Instant Messaging (IM)** e.g. sending unpleasant messages in real-time conversations on the internet.
- **Websites** e.g. insulting blogs, personal websites, social networking sites and online personal polling sites.

Any incidents of online bullying will be dealt with through the College/UCEN Manchester disciplinary policy

EQUALITY, DIVERSITY AND INCLUSIVITY

Students can expect an inclusive and supportive learning environment whatever their background, and the EDI policy is available on the Intranet.

ALIGNED POLICIES, PROCEDURES AND STRATEGIES

The Manchester College/UCEN Manchester recognise the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement, we are also aware of potential risks and challenges associated with such use.

Our approach is to implement safeguards within the College/UCEN Manchester and to support staff and students to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies. In our duty to safeguard students and protect them from the risk posed by extremism and radicalisation, we will do all that we can to make our students and staff stay safe online.

This E-Safety policy should be read in conjunction with other relevant College/UCEN Manchester policies including Safeguarding & Child Protection Policy, the At Risk Policy, the IT Acceptable Use Policy, Student Behaviour, Disciplinary & Expectations Policy, EDI Policy, GDPR Guidance.

LOCATION AND ACCESS TO THIS POLICY

- Staff Intranet – The Hub
- Student Guide – The Student Hub
- College / UCEN Manchester Website