E-Safety Policy

Document Control	
Document Type:	Policy
Department:	Student Support and Experience
Relevancy:	UCEN Manchester
Owner:	Assistant Principal Foundation Learning and Student Support
Approver:	TMC Board
Published Date:	25.10.23
Version:	1
Accessible to Students	Yes
Security Classification:	Internal and External
Last Review Date:	Sept 2023
Next Review Date:	Sept 2025

Version	Date	Revisions
1.0	Sept 2023	

Contents

1. Purpose

The purpose of this policy is to:

1.1 Set out the key principles and expected standards for students in relation to IT at UCEN Manchester with respect to the use of IT-based technologies and equipment.

1.2 Safeguard and protect the students and staff in relation to unacceptable behaviours, e.g., online safety, grooming, extremism, and radicalisation.

1.3 Assist College staff working with students to work safely and responsibly with the Internet and other IT and communication technologies and to monitor standards and practice.

1.4 Set clear expectations of behaviour and/or codes of practice relevant to the responsible use of the Internet for educational, personal, or recreational use for the whole college.

1.5 Have clear structures to deal with referrals of online abuse such as cyber-bullying, sexual harassment.

1.6 Ensure that all members of the College community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken.

1.7 Follow Safeguarding / IT guidelines to prevent issues in relation to students and staff.

1.8 This policy applies to all members of UCEN Manchester community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of College IT systems, both internally and externally of the College.

2. Scope

This policy covers:

2.1 Anyone logging into any network, service, website, or portal associated with the College/UCEN Manchester

2.2 Connecting a device via the College network

2.3 Any electronic communication with a College/UCEN Manchester Student, member of Staff or contractor

2.4 From any geographic location both on Campus and off Campus.

3. Policy Validity

This policy is valid for the academic year 2023/24 and is due for review in summer 2025.

4. Responsibilities

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

4.1 All Staff

- Are responsible for ensuring the safety of students.
- MUST report any concerns or disclosures immediately to a Designated Safeguarding Lead (DSL).
- 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.

4.2 Students:

- Must follow the IT Acceptable Use guidance identified in this policy
- 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 community.
- MUST act safely and responsibly at all times when using the internet and/or mobile technologies.

4.3 Monitoring

UCEN Manchester has IMPERO which monitors, logs and reports on students and staff use of IT systems and IT network usage as part of the College'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 disciplinary process.

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

4.4 Expected Conduct and Incident Management

All users:

- Are responsible for using the College IT and communication systems in accordance with the relevant Acceptable Use Policy/Guidance
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences.
- Understand it is essential to reporting any form of abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good online safety practice when using digital technologies in and out of College.
- Know and understand College policies on the use of mobile and handheld devices including cameras, tablets (iPads and other related equipment) and mobile phones.

4.5 Staff, Volunteers and Contractors

- Know to be vigilant in the supervision of students at all times, as far as is reasonable, and use common-sense strategies in learning resource areas where older students have more flexible access.
- Know to take professional, reasonable precautions when working with students, previewing websites before use; using age-appropriate search engines where more open Internet searching is required with vulnerable individuals.

4.6 Parents/Carers

- Should know and understand that the College has rules and guidelines for the appropriate use of IT and will take appropriate action when required.

4.7 Incident Management:

UCEN Manchester will:

- Ensure strict monitoring and application of the online safety policy and action will be taken as necessary. All members of the College are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the College's processes.
- Utilise support that is actively sought from other agencies as needed (e.g., the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues.

- Monitor and report online safety incidents and contribute to developments in policy and practice in online safety within the College.
- Ensure that Parents/Carers are specifically informed of online safety incidents involving young people when appropriate.
- Alert the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.
- Immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform other appropriate authorities including Channel as necessary.

4.8 Social Media and Safety Online

Social media is a useful tool and UCEN Manchester understand that students communicate via services such as Instagram and Snapchat. However, there are also risks attached to the use of social media and students are expected to use it responsibly whilst connected to the College network whether this be on a College device or a personal device.

4.8a **All users must adhere to the following guidelines** when accessing social media sites through the College network or on College premises.

- Use of sexually explicit language or viewing, creation or sharing of sexually explicit imagery is not permitted nor advised from a safeguarding perspective.
- Verbally abusive or threatening language is not tolerated; Use of racist or extremist language which would directly contravene British and College values, as detailed in the Prevent strategy, is not permitted.
- Use of social media for the purposes of radicalisation or the expression of extremist views is not permitted.
- Communication with staff members unless on a College established social media site is not permitted. Any such communication instigated by staff members to a student's personal social media should be reported to safeguarding team.

4.8b **Guidance for all users:**

- Don't post anything on social media that you wouldn't want others to see.
- Remember what you post could impact on your future career.
- Don't be pressured into doing anything inappropriate on social media like posting photos or videos.
- Don't accept people as friends or engage in conversations on social media if you don't know the people you are communicating with, be aware of "stranger danger".

4.8c **Keeping safe online**

UCEN Manchester encourages all students to make good use of online resources including social media. The Internet can be a rich source of information and a great way to network; however, it is important that this is done safely.

Below is some guidance about how to work online safely:

- It is a warning sign if someone only wants to talk to you in secret and they are asking you not to tell anyone about your conversations.
- Never agree to talk to anyone in secret, especially if they are threatening you not to tell anyone about it. Always inform a trusted adult of your online conversations.
- It isn't OK for someone online, who you don't know, to insist on taking your phone number or address.
- Never give out personal details such as your name, address or phone number and never tell anyone which school/college you go to. Keep your personal details private. In the wrong hands, these details can be used to find you, meaning you may become at risk.
- If you are sent an email that makes you feel uncomfortable or worried speak to a member of college staff or contact the Pastoral Hub. For example, the person emailing you may say things or send you embarrassing/inappropriate pictures.

In addition, the person could be insisting that you use a webcam or send them photographs of yourself that make you feel uncomfortable.

This is never OK, and you should never send anyone, including those you met online, photo of yourself that may make you feel uncomfortable.

- Always tell a trusted adult if someone makes inappropriate comments or suggestions or makes you feel uncomfortable.
- Never agree to meet anyone you have met online on your own. Only meet someone you have met online in a public place with one of your parents or another trusted adult.

4.8d **The risk of radicalisation online**

Extremist groups are known to use the internet and social media to communicate with vulnerable young people and spread radical messages, aiming to gain more recruits and supporters. When the internet is used safely and responsibly, there are lots of positive opportunities for people to learn so it's important to be aware of negative influences online.

Keep safe from extremism and radicalisation online:

- Don’t view people you have encountered on social media or through online games as ‘Online friends’. They are strangers, it’s important to remember that it’s easy for people to lie about themselves online.
- Extremism comes in many forms, it doesn’t have to be in relation to skin colour, race, or religion. If someone is expressing their views in an aggressive or inappropriate manner you should disengage with this conversation and block them or report them to the Safeguarding team or the POD.
- Do not follow or like extremist groups on social media, this provides them with opportunities to contact you to express extreme views.
- Do not force your opinions or views on others online, this can be classed as extremist and may make others feel uncomfortable.
- Hate language such as homophobic, transphobic, or racist insults is inappropriate and extreme. You do not have to accept it and you should report this to the Safeguarding team or the Pastoral Hub. If you are concerned about anything you encounter online, you can seek help and support from staff in the Pastoral Support Hub

Useful websites to help you learn more about online safety. If you are concerned about something, you can call the NSPCC’s online safety helpline on 0808 800 5002.

Additional resources can be found here:
http://educateagainsthate.com/parents/online-radicalisation
https://www.childnet.com/resources/supporting-young-people-online

5. Roles and Responsibilities

5.1 Student Experience and Support Department

The **student experience and support department** is responsible for the review and updating 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 Committee meetings
- Regular monitoring of e-Safety incident logs - via monitoring software reporting and feedback at department meeting agendas from Heads of Safeguarding and Pastoral Support
- Heads of Safeguarding and Pastoral Support have a duty of care for ensuring the safety (including e-Safety) of students, though the day-to-day responsibility for safety.
- The Assistant Principal and Heads of Safeguarding and Pastoral Support will ensure that there is a system in place to allow for monitoring and support of those in College 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.

5.2 Head of Safeguarding and Pastoral 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 technical staff.
- receives reports of online safety incidents from Impero and creates a log of incidents.
- attends relevant meeting reports regularly to College Leadership Team where appropriate.

5.3 Director of IT / Technical staff:

- The College has a managed ICT service provided by LTE Group Operations. The LTE Group IT Services team will work with the College to ensure all online safety measures are implemented in collaboration with the college safeguarding team, ensuring the College'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 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. All students have appropriate access to systems they require using their own device both on the College WIFI and over the internet.
- Any personal device connected to UCEN MANCHESTER systems will be logged and monitored for security and audit purposes. Information such as the make and model of the device as well as details of the software installed on it will be visible to the IT team.

- When using UCEN MANCHESTER networks such as BYO and library systems, the use of VPNs to bypass filtering and security controls is strictly prohibited. Continued use of VPN software will result in the users' access to UCEN MANCHESTER digital resources being withdrawn

5.4 Quality Team

Group Quality Manager (Digital Lead) will develop and implement the Digital Learning strategy for 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.

5.5 Safeguarding Strategy Group

The Safeguarding Committee 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

5.6 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.

5.7 Blended Learning

For some courses there may be some element of blended learning. When accessing learning from home please makes sure you follow the below:

- Identify a quiet space at home to work in
- Think about your surroundings.
- If possible, work at a desk
- Either blur or use an effect background so that those you are working with online cannot see your surroundings
- Be professional at all times.

- If you have any concerns about your blended learning experience, please contact your tutor or one of the safeguarding team.

5.8 Do's and Do Nots

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

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

5.8a **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 devices may, on occasion, be used to gather either video or photographic evidence in order to support students' course requirements provided that the College 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 intensions for example to intimidate or to extract financial information for personal gain. All conversations using College IT systems are captured and recorded on the College's servers.
14. You must not post any confidential information to any online platform.

5.8b **If your post could be considered as representing or being associated to the College in any way, then:**

1. It is imperative to portray a balanced tone when raising politically sensitive issues.
2. When linking to websites not controlled by the College (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 user account these include:
3. Email (using a College email address)
4. SMS (using a College device).
5. Microsoft Teams and Microsoft Office 365 collaboration (using a College account)

6. Training

6.1 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 radicalisation and in personal, social and health 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.

6.2 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 Keeping Children Safe in Education statutory guidance (KCSiE) with mandatory sessions logged within HR.

7. 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.

8. Aligned Policies, Procedures and Strategies

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 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.

Related Policies and Documents

- Safeguarding Policy
- IT Acceptable Use Policy
- Disciplinary Policy (staff and students)
- Data Protection Policy

Location and Access to this Policy

- Staff HUB
- Student HUB