MacIntyre Academies
Quest Academy

Online Safety Policy (formerly e-Safety Policy)

Version:	Changes/Updates	Responsibility:	Date:
V4	Rephrased throughout. Changed from E-Safety to Online Safety. Smart watches not permitted to align with Behaviour Policy. YouTube and other such sites not accessible unless done so with direct supervision.	T Owen	Sept 2025

Person Responsible:	Principal
Type of policy	Non-statutory
Date of first draft:	May 2022
Date of staff consultation:	
Date adopted by the LAB:	December 2022
Date of implementation:	December 2022
Date reviewed:	September 2025
Date of next review:	September 2026

Contents

Introduction

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance Keeping Children Safe in Education, and other advice on teaching online safety, preventing and tackling bullying and cyber-bullying, and protecting children from radicalisation. It also reflects the Education Act 1996, Education and Inspections Act 2006, Equality Act 2010 and Education Act 2011. The policy takes account of the National Curriculum computing programmes of study, and complies with our funding agreement and articles of association.

Quest Academy, as part of MacIntyre Academies Trust (MAT), recognises that the Internet, and access to it via a range of technologies, is an attractive and increasingly integral feature of learner's learning and entertainment. The Academy recognises too, that in enabling access to this invaluable resource it has a duty to ensure that learners are:

- Safe from inappropriate content in a range of forms and across technologies
- Safe from bullying and harassment of any kind
- Safe from crime and anti-social behaviour in and out of the Academy and Trust
- Secure, stable, and cared for while online

It is the duty of the Academy to ensure that every learner in their care is safe, and that the same safeguarding principles should apply to the 'virtual' or digital world as would be applied to physical buildings.

This Policy document has been drawn up to protect all parties – the learners and the staff and aims to provide clear advice and guidance on how to minimise risks. It has been written alongside the MAT Acceptable Use of ICT Policy (AUICT) and the MAT Social Media Policy.

Research has proven that the use of technology brings benefits to learning and teaching. However, as with many technological developments, there is also an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help learners to develop the skills and confidence to manage potential risks and considerably reduce their impact. It will also ensure that staff members working at the Trust are aware of how to protect learners against such risk, and to considerably reduce their impact.

Quest Academy's Online Safety Policy, as part of the Academies wider safeguarding agenda, outlines how we will ensure our learners are prepared to deal with the safety challenges that the use of technology brings.

Our approach to online safety is based on addressing 4 key categories of risk:

- Content: exposure to illegal, inappropriate or harmful material
- Contact: harmful online interaction with other users
- Conduct: personal online behaviour that increases risk or harm
- Commerce: risks such as gambling, scams and advertising

The Online Safety Policy relates to other policies including those for Safeguarding, AUICT, and Anti-Bullying. The Designated Safeguarding Lead at Quest Academy is the Principal. There is a Safeguarding Lead on the Local Advisory Board (LAB), who has attended Online Safety training.

1. Teaching and learning

1.1 Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business, and social interaction. The Academy has a duty to provide learners with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and learners.

ICT will be used across the Academy to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences. It will also be used for enrichment opportunities within the curriculum.

1.2 Internet use will enhance learning

The Academy internet safety mechanisms will ensure that learners are protected against accessing content and information which is unsuitable and deemed to be inappropriate for their age group.

Learners will be supervised to understand what is and is not appropriate use of the internet.

Where appropriate, learners will be shown how to publish and present information to a wider audience using the internet as a tool.

1.3 Learners will be taught how to evaluate Internet content

The Academy will ensure that the use of internet derived materials by staff and learners complies with copyright law.

Where appropriate or necessary learners will be supported to know the importance of cross-checking information before accepting its accuracy and making sure it is what they need.

Learners will be taught:

- What to do if they access inappropriate content (reporting to an adult and letting an adult know they have seen something which they do not like).
- How to report unpleasant Internet content e.g., using the CEOP Report Abuse icon () with support from adults with them.
- How to tell an adult or a person supporting them that they are concerned about something which they have seen.

2. Managing Information Systems

2.1 Information system security

Quest Academy uses the MacIntyre Academies Trust ICT infrastructure. The ICT systems security will be reviewed regularly.
Virus protection will be updated regularly and assessed as appropriate for need.
The ICT systems are encrypted.

ICT security systems for the Academy will ensure that sensitive and confidential information stored on its server systems and the cloud are protected, and not accessible to the outside world through the use of the internet.

Staff are aware of and will follow the MAT Personal Data Breaches policy in the event of a data breach.

Staff have specific logins unique to themselves which will grant access to shared drives and folders.

Guests who would like to link to the internet whilst visiting the academy site will be permitted to do so through the guest internet log in, which is secure and does not give access to shared drives and folders which may contain sensitive information.

The Academy has access to an internet filtering system which allows internet use to be monitored and reviewed at any time – trends and content of websites can be seen under each individual person's (adult and learner) login details. The family footings team and the deputy DSL have responsibility for monitoring this on a weekly basis and any concerns are raised at the Senior Leadership Team meetings, and a plan of action taken forward to support the investigation of this if needed.

Users must use strong passwords. A strong password must: 1. Be long (8 or more characters) 2. Include a range of characters, such as: Upper case and lower-case letters, numbers, punctuation marks and

other symbols 3. Not contain single dictionary words, where possible. Note that phrases or two words together is better. 4. Not include simple substitutions of characters, e.g., "p4$$w0rd" 5. Not include patterns derived from the keyboard layout, e.g., "qwerty" 6. Not use obvious choices of passwords.

Passwords may be saved as per the MAT Acceptable Use of ICT Policy (AUICT).

Password sharing for systems that protect personal data is not allowed. Sharing accounts, or even occasional use by anyone other than the account holder, negates the benefit of authenticating a specific user. In particular, the ability to audit and monitor a specific user's actions is lost.

2.2 E-mail

Learners may only use approved email accounts which are assigned to them as individuals. This may be restricted and/or deactivated where necessary. For example (not limited to) , whereby a learner is using this to contact staff outside of school hours.

Confidential/sensitive information will be sent encrypted using Egress Switch to those agencies outside of the Academy who managers and staff need to share information about learners with.

Staff will ensure that in email communication, learners must not reveal their personal details or those of others or arrange to meet anyone without specific permission. All learners will be supported to use their email accounts appropriately.

The forwarding of chain letters is not permitted, and staff are aware of this.

Incoming email should be treated as suspicious, and attachments not opened unless the author is known.

The Academy will consider how email from learners to external bodies is presented and how this is checked to ensure it is being sent to an appropriate receiver.

Staff will support all learners when they are using email, at all times. As a result, if any offensive emails which are witnessed by staff members as having been received by a learner, these will be noted and reported to a member of the Senior Leadership team Team.

If a user receives an email in error, they should inform the sender and delete the email. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

Staff members all have their own log-in details and passwords which are unique to them. Sharing log in and password information is prohibited.

2.3 Published content and the Academy web site

The contact details given on the website will be the Academy address, email, and telephone number. Staff or learner personal contact information will not be published.

The Senior Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing learner's images and work

Written permission will be sought from parents/carers before photographs of learners are published on any of the Trusts websites.

Learners' full names will not be used anywhere on the Trust websites or other online space (such as X (previously twitter), particularly in association with photographs.

Leaner image file names will not refer to the learner by name.

Parents/carers should be clearly informed of the Trusts policy on image taking and publishing, both on Trust and independent electronic repositories.

A current list will be kept and updated to show the permissions given by parents/carers for learners' images to be published on the main website.

2.5 Social networking and personal publishing

Learners will be advised and supported by staff to never give out personal details of any kind which may identify them, their friends, or their location through social media.

Staff are not to discuss any confidential information about the Trust on their own social networking sites. Staff are to remember that they are representing the Trust in a professional light at all times and that their conduct in online forums also reflects their professionalism.

Staff are not to contact learners, parents/carers, or family members on social networking sites.

Learners and parents/carers will be advised that the use of social network spaces outside the Academy brings a range of dangers for learners and that these are to be carefully monitored.

Where parents/carers share that their learner has a profile on a social networking site, it will be made clear that the Academy can advise parents/carers on how to make sure that their learner is safe online should they wish for support with this.

The Academy will work with Social Care and families to make sure that devices learners use (such as iPads and Kindles) can be safely monitored through parental controls, should parents/carers want advice on this.

2.6 Managing filtering

The Trust will work with appropriate agencies and partners to ensure systems to protect learners are reviewed and improved.

If staff or learners come across unsuitable online materials, the site must be reported to the Academy IT Technician or School Business Manager immediately. Should there be a need to report this further, then appropriate advice will be sought.

2.7 Managing video conferencing & webcam use

The use of webcams can only be used with the permission of the Principal or other the Senior Leadership Team.

Webcams will only be used on central computers and laptops, of which all staff members are aware. Their use will not be permitted through the use of guest computers or laptops.

Teams/Zoom

Teams/Zoom is an important way for staff to communicate with other staff and to keep in touch with parents/carers and families.

Staff members will ensure that they have checked the Teams/Zoom link before they access a Teams/Zoom meeting.

If a call is made to parents/carers then they will be asked for permission for their Teams\Zoom contact addresses to be used.

Recordings should not be made of any Teams/Zoom meeting involving a learner or staff member without their permission. Any recordings made need to be deleted after use.

The calls made via Teams/Zoom will be on the Trust network with content filters in place.

2.8 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use at the Academy is allowed.

Mobile phones are not permitted to be used at any of the Trust Academies when working with learners as per the MAT Acceptable Use of ICT policy.

Learner's mobile phones must be handed in to appropriate staff when entering the Academy. These will be given back at the end of the day as they leave.

Staff mobile phones may be taken by staff on trips to use in emergencies, and this is always written up in the risk assessment. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The use by learners of cameras in mobile phones will be kept under review. Staff are not permitted to use the cameras on their phone to take photos of learners or staff for any means.

Games machines including the Sony PlayStation and Microsoft Xbox, potentially have Internet access. Staff will supervise learners who access such devices and ensure that the internet access is not available, unless this is used to access an online game with appropriate school agreed restrictions in line with our AUICT Policy.

Learners will be supervised when using computers and laptops. Devices are monitored on our network and internet activity is recorded. Staff will ensure reasonable measures are taken when learners are accessing online games such as restricting chat use as well as other school agreed restrictions in line with our AUICT Policy.

iPads/Kindles and access to wireless internet use on such devices is continually monitored, and all wireless access for such devices is controlled through the Trust account and guest account.

Learners with watches that can connect to the internet, receive and make calls, take and store images and sound recordings are not permitted in line with our Academy Behaviour Policy. Their personal mobile phones that would be their own connection opportunity will be securely stored to prevent unauthorised use.

AI Chat Bots are blocked by our web filtering security to prevent use by any learner.

2.9 Protecting personal data
Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998.

3. Policy Decisions

3.1 Authorising Internet Access
The Academy will maintain a current record of all staff and learners who are granted access to Trust ICT systems.

Any person not directly employed through the Trust who requires access to the wireless internet connection will be asked to use the Guest account and log in details, and this will be monitored by security systems for access to inappropriate content.

3.2 Assessing risks
The Trust will take all reasonable precautions to prevent access to inappropriate material, including providing appropriate close supervision. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Trust network. The Trust cannot accept liability for any material accessed, or any consequences of Internet access.

Planned, regular training will be available to staff teams to ensure their understanding of the associated risks linked to online safety and course of action needed if they are concerned about any content which they or a learner has seen.

All staff will be required to complete a cyber security module as part of the e-learning package available.

Identified risks will be reported and a course of action outlined to ensure that the inappropriate content cannot be viewed again.

3.3 Handling e-Safety complaints
Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Senior Leadership Team.

Complaints of a child protection nature must be dealt with in accordance with the Quest Safeguarding Policy.

Learners and parents/carers are informed of the complaints procedure and how to make a complaint should they need to do so.

Complaints will be logged and monitored by the Senior Leadership Team and information shared with appropriate agencies involved with individual learners such as Social Care and CAMHS where a multi-agency working approach is in place.

Advice around who to contact to make records of complaints will be sought in line with Safeguarding procedures at Warwickshire Safeguarding Executive Board and Warwickshire County Council.

4.Communications Policy

4.1 Introducing the e-Safety policy to learners

Learners will be informed that network and Internet use will be monitored and appropriately followed up. Staff working with learners are required to reinforce this through supervision and monitoring of learners when they use the internet. Learners will be informed that any devices they access are the property of the Trust.

Online Safety training will be embedded within the ICT scheme of work and the PSHE Curriculum.

4.2 Curriculum

Pertinent and relevant information as appropriate for the learner's cognitive understanding will be shared and taught.
Learners will not have direct access to 'YouTube' and other such sites, where this accessed, will be directly supervised by a member of staff. Learners will be encouraged to understand that some of the content of these sites is not available for their use and will be blocked in accordance with Trust policies.

4.3 Staff and the Online Safety policy

The Online Safety Policy and MAT AUICT Policy is given to each staff member as part of their induction, and they must read and sign to say they understand and agree with the policy.
Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
Staff will always use a child-friendly safe search engine when accessing the web with learners.
Staff will be supported to understand what it means to be 'safe' on the internet, and in the context of learners with Special Educational Needs accessing and using the internet.

4.4 Enlisting parents' and carers support

Parent and carers attention will be drawn to the Academy Online Safety policy and to the Academy website.
The Academy will maintain a list of Online Safety resources for parents/carers and share these as appropriate.
Links to further safety information will be shared on the Academy website.
Sites of use for parents, carers, staff members and learners can be found below:

- http://www.ceop.police.uk/
- http://www.thinkuknow.co.uk/
- https://www.warwickshire.gov.uk/keeping-child-safe/cyber-safety/1
- https://www.warwickshire.police.uk/police-forces/warwickshire-police/areas/warwickshire-police/campaigns/campaigns/2019/be-cyber-smart/
- http://www.childnet.com/

Changes at previous reviews:

Version:	Changes/Updates	Responsibility:	Date:
2	Removal of staff names Update password saving as per MAT Acceptable Use of ICT Policy (AUICT) 5.2 – paragraph given the subheading ‘curriculum’.	V Scranage	July 23
3	E Safety training updated to cyber security	V Scranage	July 24