MacIntyre Academies
Venture Academy

E-Safety Policy

Version	Purpose/Change	Responsibility	Date
1	New Policy	Executive Principal	Dec 2024
2	Policy review Terminology changed from children/young people/pupils to learners throughout 3.6 - 'Studybugs' removed 3.9 - Post-16 line removed Appendix 1 – Staff list updated	Principal	Dec 2025

Person responsible:	Principal
Type of policy:	Non-Statutory
Date of first draft:	Sep 2024
Date approved by LAB:	Dec 2024
Date reviewed:	Nov 2025
Date of next review:	Dec 2026

E-Safety Policy Contents

E Safety Policy

Venture Academy, part of MacIntyre Academies, educates and supports learners with diagnoses of Autism (ASC) and/or with Social, Emotional or Mental Health Needs.

1. Other relevant policies

This policy must be read in conjunction with:

- Venture Academy Safeguarding Policy and Procedures
- Venture Academy Mobile Phone Policy (learners)
- MAT Code of Conduct
- MAT Acceptable Use of ICT (AUICT) Policy (staff and volunteers)
- MAT Data Protection Policy

2. Purpose

The purpose of this policy is to:

- Ensure the safety and wellbeing of learners is paramount when adults, young people, or children are using the internet, social media or mobile devices
- Provide staff and volunteers with the overarching principles that guide our approach to online safety
- Ensure that, as an academy, we operate in line with our values and within the law in terms of how we use online devices.

We believe that:

- Learners should never experience abuse of any kind.
- Learners should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.
- Parents/carers and other agencies are critically important in ensuring this happens out of school time too.
- All learners, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

1. Introduction

Information & Communication Technology (ICT) is an essential element of 21st century life for education, business and social interaction. The opportunities provided by the internet are tremendous, both within school and outside.

However, the internet has bought with it new ways to hurt and abuse, (including through cyberbullying, online grooming and sexual abuse of children). Therefore, schools have a safeguarding responsibility and a duty of care to provide learners with good quality and safe internet access as part of their learning experience and to do their best to educate learners about the risks that the online and e-communications landscape can bring.

The E-Safety Policy encompasses not only the Internet but also wireless electronic communications including mobile phones, smart watches, game consoles and cameras. It highlights the need to educate learners about the benefits, risks and responsibilities of using ICT.

The aim is to provide safeguards and raise awareness, which will enable users to control their online experiences and feel confident and happy using technology. Individuals will learn about laws and statutory guidance that relate to e-safety, including the Online Safety Bill 2023, a new set of laws that protects children and adults online. The new Bill puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms.

2. Teaching and Learning

2.1 Why the internet and digital communications are important

- Internet use is a part of the statutory curriculum and a necessary tool for staff and learners.
- Some of the many benefits of using the internet include:
  - Access to a wide variety of educational resources including art galleries, historical sources, maps and information.
  - Rapid world-wide communication
  - An increased understanding of people and cultures around the world
  - Increased skills across the curriculum and in improving research and communication skills
  - Staff professional development

2.2 Internet provision

- Learners are taught about which aspects of internet use are acceptable and what is not as clear objectives for internet use.
- Learners are helped to understand age-appropriate content and the bodies that recommend/determine age restrictions.
- Learners are educated in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation.
- Learners are shown how to publish and present information appropriately to a wider audience.

2.3 Learners with Special Educational Needs

The school recognises that certain aspects of E-Safety are particularly challenging for learners with special educational needs. Individuals who have poor social skills may be more at risk from inappropriate online contact. We minimise this risk through learning about the risks at a level our learners can understand and modelling good practice as adults. We additionally ensure that equipment and software provided by the Academy is set up to protect learners as much as possible. We do not allow learners to have their own handheld devices in the building to reduce the risks of photography and associated risks with filming other learners.

3. Managing E-Safety

3.1 System Security

- School ICT systems security will be reviewed regularly
- Virus protection will be up-dated regularly
- Security strategies will be discussed with the Local Authority and agreed with the Local Advisory Board

- The academy uses a firewall 'Smoothwall' which is managed by the academy in partnership with the provider of ICT, the prohibitions list is regularly updated to reflect current contextual trends in safeguarding
- The academy uses 'Impero' software to monitor pupil activity on academy devices used on the network

3.2 Accessing the Internet

- The internet is regularly used by teachers/staff as a planned part of lessons/sessions.
- All staff will review and evaluate resources on websites appropriate to the age range and ability of the learners being taught.
- It is important that staff check that online resources remain age appropriate e.g., that the adverts around a certain clip are still age appropriate or that the music on the soundtrack is age appropriate
- Access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
- As they gain experience, learners become more independent, using searching techniques to locate information for themselves. An adult will always be present to supervise, however the teaching staff's attention cannot be on every screen at all times.
- Learners are taught to be critically aware of the materials they read, and that they might need to validate information before accepting its accuracy.
- Learners will be taught how to report unpleasant Internet contents e.g., using the CEOP Report Abuse icon
- The school is aware that some Internet derived materials may have restricted access due to copyright law, and staff must comply with such law.
-

3.3 E-mail

Learners will be taught:

- To exchange information via-e-mail, to use an address book, to attach files to an e-mail.
- To follow conventions of politeness.
- To tell a member of staff if they receive offensive e-mail.
- To not reveal personal details of themselves or others in e-mail communication, without specific permission.
- To treat all in-coming e-mail with some suspicion, not opening attachments unless the author is known.
- How to present e-mails to external bodies
- That forwarding of chain letters is not permitted.
- Email communication between staff and learners must only take place via a school email address or from within the learning platform. For example, staff members must not share personal email addresses or contact information or accept children onto their Facebook accounts.

3.4 Publishing learners' images and work

- Parental permission is gained before images/photos of learners are published on the school website or on the school learning platforms.

3.5 The School Website (www.ventureacademy.org)

- The contact details of Venture Academy website will be the school address, e-mail and telephone numbers of the Academy and the residential buildings. Staff or learners' personal information will not be published

- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include learners will be selected carefully, taking account of the written parental/carer's consent.
- Learners' full names will be avoided on the website.

3.6 The MacIntyre Academies' Learning Platform is Microsoft Office with tools such as Class Dojo also being implemented.

- The school's learning platform is password protected, with different levels of security being available to different users.
- Learners will be taught safe use of the school learning platform, before they are allowed to use it.
- Online forums within the learning platform are set up and managed by staff only
- Photographs that include learners will be selected carefully, taking account of the written parental/care's consent, prior to any publication
- As the platform technology advances, the person responsible for ICT will ensure that all users are aware of the impact of these advances.

3.7 Social Networking

- There will be no access to social networking at the academy other than facilitation of discussions or virtual learning through Microsoft Office tools.
- Learners and parents will be taught about the dangers that the use of social network sites outside school bring.
- Learners will be advised to use nicknames and avatars when using social networking sites out of school
- Learners will be taught never to give out personal details of any kind which may identify them or their location (including sharing their location from a mobile device), or post personal photographs.

3.8 Managing filtering

- If staff or learners come across unsuitable on-line materials, the site must be reported to The IT team and the IT helpdesk.
- Teaching staff will monitor that the filtering methods selected are appropriate, effective and reasonable.
- Where a learner is known to have accessed inappropriate material in or out of school this should be logged on the safeguarding system and/or shared with a Designated Safeguarding Lead as soon as possible.

3.9 Other Technologies

- Staff will use a school phone for all normal contact with parents/carer's homes. Personal mobile phones will not be used during lessons or formal school time. Personal mobile phones may be required on trips outside the school to contact the school office. They may also be used under exceptional circumstances with the permission of the Principal to call parents/ carer's emergency contact numbers directly, but staff should withhold their contact number if this is needed
- The sending of abusive text messages or harmful content must be discouraged and reported
- The academy is aware that as learners become more independent in Upper Key stages, they may bring mobile phones onto the school site. All mobile phones will be locked away in the office during the school day.

- Personal cameras, or cameras on mobile phones will not be used for school business. School cameras will always be used.
- Images of children must not be down-loaded onto personal devices; they must be down-loaded to the school system and kept on the school premises.
- Game consoles (including Play-station, X Box, WII and others) will be part of activity and reward programmes; they will be carefully monitored for age-appropriate games and filtering. They will not be used on the school Wi-Fi system other than to be updated.
- Emerging technologies / communication aids will be examined for educational benefit and assessed for risk, before use in the school.

3.10 Use of School equipment for home use

- Academy equipment must be used only for school business.
- When a laptop or device is taken home it must only be used by the member of staff to whom it is allocated, passwords must never be shared with anyone else. (Refer to MAT Acceptable Use of ICT Policy)
- School devices must not be left unattended in public spaces or in a vehicle.
- Where learners have a school device at home, it must be set up on the school system and subject to the usual filtering and virus protection. It is incumbent on adults in the home of a learner with a school laptop to supervise them online and ensure their safety when they are using a device.
- Both members of staff and students need to be aware that access to the wider internet at home increases the possibility of virus attack and potential theft.
- School laptops may not be used for illegal or inappropriate material, illegal material includes possessing or distributing indecent images under 18, illegally downloading music etc. Inappropriate material includes accessing adult pornography; ‘put downs’ on the basis of race, religion or orientation etc.; harassing or threatening individuals; making derogatory, offensive or insulting comments about learners or colleagues.
- Staff need to be aware of the risks involved in storing and transporting confidential information. The safest storage location is the school network.

3.11 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Our Data Officer is Jennie Nicholls, and she oversees how we hold and process data

4. Policy Decisions

4.1 Authorisation of access to the ICT system. In accordance with the Acceptable Use of ICT Policy:

- All staff and governors must read and sign the Acceptable Use Agreement and the MAT Code of Conduct before using any school ICT resource.
- The academy, and the Trust ICT provider will maintain a current record of all staff and learners who are granted access to school ICT systems.
- Learners will have been informed of the school’s ICT rules and E-Safety guidance.
- Any person not directly employed by the school will only be allowed access to the school network at the discretion of the Principal.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material, however due to the international scale and linked internet content it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Whilst we will take all reasonable measures, neither the school nor MacIntyre Academies Trust can accept liability for the material accessed, or any consequences of Internet access.

4.3 Responding to an E-Safety incident

- Complaints about internet misuse by learners will be dealt with by a member of the senior leadership team (or delegated to a DSL) and will follow the school's appropriate policy and outcomes.
- Learners and their parents/carers will be informed about any complaint's procedures and the consequences for learners misusing the Internet.
- Any complaints about staff misuse must be referred to the Principal.
- Any Concerns about the Principal should be referred to the Group Director for MacIntyre Academies Trust.
- Complaints of a safeguarding or child protection nature must be dealt with in accordance with school child protection procedures.
- The Academy will refer any incidents of the sharing of child pornography, revenge porn persistent online harassment to the Integrated Front Door or directly to the police, in accordance with the Safeguarding policy.

4.4 Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-Safety Policy.
- Visitors with appropriate roles may only use the guest Wi-Fi on site and not the internal Wi-Fi system.
- The password for the Wi-Fi system will not be shared.

5. Communications

5.1 Sharing the E-Safety Policy with Learners

- Appropriate elements of the E-Safety Policy will be shared with learners.
- E-Safety rules will be visible in all networked rooms
- Learners will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-Safety issues and how best to deal with them will be provided for learners in appropriate communication formats.
- Opportunities like Safer Internet Day will also be used as a reminder to learners about safe use of systems and devices.

5.2 Sharing the E-Safety Policy with staff

- All staff will have access to the E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Direction and professional conduct are essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the senior leadership team and have clear procedures for reporting abuse.

5.3. Sharing the E-Safety Policy with parents. Enlisting parents' support.

- Parents and carers attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school website.

- Parents and carers will from time to time be provided with additional information on E-Safety.
- The school will ask all new parents to sign the parent/young person agreement when they register their child with the school.

6. Statutory Context of E-Safety

This section included some of the statutory context surrounding E-Safety.

- E-Safety falls within the remit of “Keeping Children safe in Education” 2022.
- Behaviour in Schools (2022) gives advice to school leaders about how to manage behavioural issues that might arise in schools. This guidance may be particularly important when dealing with E-Safety issues; online bullying may take place both inside and outside school, and this legislation gives the school the legal power to intervene should incidents occur. It also gives schools the powers of search, to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.
- Online Safety Bill 2023 – Social Media platforms will be required to prevent children from accessing harmful and age-inappropriate content and provide parents and children with clear and accessible ways to report problems online when they do arise.

Appendix 1

Key Personnel

Academy ICT Lead:
Jennie Nicholls, School Business Manager

The Designated Safeguarding Leaders are:

- James Bowater - Principal
- John Anderson – Assistant Principal
- Layla Shepherd – Assistant Principal
- Shelley Molloy – Assistant Principal
- Jennie Nicholls – School Business Manager
-
- Kirsty Caudell – Compassionate School Coach
- Katie Thomas – Positive Behaviour Coach
- Tom Manise – Outreach Worker
- Emma Day – Family Footings Facilitator
- Sam Townsend – Designated Teacher for LAC