MacIntyre Academies
Discovery Academy

E-Safety Policy

Version	Purpose/Change	Responsibility	Date
4	Section 3.6– Software/Programmes updated to reflect current systems Section 6– KCSIE “024 and Behaviour in Schools 2024 and added reference to the Online Safety Act 2023 Appendix 1 – Updated Roles and Responsibilities	Principal	June 2025

Person responsible:	Principal
Type of policy:	Non-Statutory
Date of first draft:	July 2015
Date approved by LAB:	April 2023
Date reviewed:	June 2025
Date of next review:	June 2026

E-Safety Policy

Contents

Discovery Academy, part of MacIntyre Academies, educates and supports children and young people with diagnoses of Autism (ASC) and/or with Social, Emotional or Mental Health Needs.

Other relevant policies

This policy must be read in conjunction with:

- Discovery Academy Safeguarding Policy and Procedures
- Discovery Academy Mobile Phone Policy (children and young people)
- MAT Code of Conduct
- MAT Acceptable Use of ICT (AUICT) Policy (staff and volunteers)
- MAT Data Protection Policy

Purpose

The purpose of this policy is to:

- ensure the safety and wellbeing of children and young people 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:

- Children and young people should never experience abuse of any kind.
- Children 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 children, 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 students with good quality and safe internet access as part of their learning experience and to do their best to educate children and young people 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 children and young people 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.

2. Teaching and Learning

2.1 Why the internet and digital communications are important

- Internet user is a part of the statutory curriculum and a necessary tool for staff and young people.
- 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

- Young people will be taught about which aspects of internet use are acceptable and what is not as clear objectives for internet use.
- Young people will be educated in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation.
- Young people will be shown how to publish and present information appropriately to a wider audience.

2.3 Children and young people with Special Educational Needs

- The school recognises that certain aspects of E-Safety are particularly challenging for young people with special educational needs. Children 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 children and young people can understand and modelling good practice as adults. We additionally ensure that equipment and software provided by the Academy is set up to protect children and young people as much as possible. We do not allow children and young people to have their own handheld devices in the building to reduce the risks of photography and associated risks with filming other children.

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 young people 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, young people 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.
- Young people are taught to be critically aware of the materials they read, and that they might need to validate information before accepting its accuracy.
- Young people 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

Young people 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 young people 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 young people images and work

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

3.5 The School Website (thediscoveryacademy.org)

- The contact details of Discovery Academy website will be the school address, e-mail and telephone numbers of the Academy and the residential buildings. Staff or young people personal information will not be published
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include young people will be selected carefully, taking account of the written parental/carer's consent.
- Young people full names will be avoided on the website.

3.6 The MacIntyre Academies' Learning Platform is Microsoft Office with tools such as Class Charts and Study Bugs also being implemented.

- The school's learning platform is password protected, with different levels of security being available to different users.
- Children and young people 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 children and young people 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.
- Young people and parents will be taught about the dangers that the use of social network sites outside school bring.
- Young people will be advised to use nicknames and avatars when using social networking sites out of school

- Young people 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 children and young people 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 pupil 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 and or Class Charts messaging app 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 children and young people become more independent in Upper Key stages, they may bring mobile phones onto the school site. All mobile phones will be locked away in their classroom / offices / medical cabinet during the school day.
- Students in post-16 are able to check their mobile phone with staff supervision in the school day by prior agreement
- 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 children and young people 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 pupil 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 young people 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 2018.
- Our Data Officer is Peter Merrylees, and he oversees how we hold and process data.

4. Policy Decisions

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 young people who are granted access to school ICT systems.
- Young people 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 Executive Principal / Head of School.

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.

Responding to an E-Safety incident

- Complaints about internet misuse by young people will be dealt with by a member of the senior leadership team (or delegated to a DSL) and will follow the schools appropriate policy and outcomes.
- Children or young people and their parents/carers will be informed about any complaint's procedures and the consequences for young people 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.

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

Sharing the E-Safety Policy with Children and Young people

- Appropriate elements of the E-Safety Policy will be shared with young people.
- E-Safety rules will be visible in all networked rooms
- Young people 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 young people in appropriate communication formats.
- Opportunities like Safer Internet Day will also be used as a reminder to children and young people about safe use of systems and devices.

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” 2024.
- Behaviour in Schools (2024) 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.
- The Online Safety Act 2023 Online Safety Act: explainer - GOV.UK

Changes at previous reviews:

Version	Purpose/Change	Responsibility	Date
3	The policy has been significantly updated to reflect current practice	Executive Principal	April 2023

Appendix 1

Key Personnel

Academy ICT Leads:

- Mark Hardy is Lead Teacher for ICT and oversees the operational aspects of our system and its protections.

The Designated Safeguarding Leaders are:

- Tony Leigh – Principal
- Lorraine Nicholls – Safeguarding Lead
  - Lauren Ault – Assistant Principal
  - Matt Clark – Assistant Principal
  - Jinny Cumiskey – Assistant Principal
  - Chris Harlan-Marks – Assistant Principal