MacIntyre Academies
Discovery Academy

E Safety Policy

++

E Safety Policy
Adopted by Trust Board: July 2015
Review by LAB: February 2019
Next Review: February 2021

E-Safety Policy

1. Introduction

Information & Communication Technology (ICT) is an essential element in 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.

The E-Safety Policy encompasses not only the Internet but also wireless electronic communications including mobile phones, 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

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.

2.2. Children 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.

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.

3.2. Accessing the Internet

- The internet is regularly used by teachers as a planned part of many lessons.
- All staff will review and evaluate resources on websites appropriate to the age range and ability of the young people being taught.
- 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 accept children onto their Facebook accounts.

Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role.
Adults should ensure that all communications are transparent and open to scrutiny. (Guidance for Safer Working Practice for Adults Who Work with Children and Young People, 2007)

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 platform.

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

- The school's learning platform is password protected, with different levels of security being available to different users.
- Young people will be taught safe use of the school learning platform, before they are allowed to use it.
- The school's E-Safety rules will be published on the school learning platform which contains a link to the CEOP website, explaining how children and young people can report incidents that they feel concerned or uncomfortable online.
- Online forums within the learning platform are a means of facilitating discussion of E-Safety.
- Photographs that include Young people will be selected carefully, taking account of the written parental/care's consent.
- 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.

- 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.
- Young people will be taught never to give out personal details of any kind which may identify them or their location, or post personal photographs.

3.8. Managing filtering

- If staff or Young people come across unsuitable on-line materials, the site must be reported to a member of teaching staff.
- Teaching staff will monitor that the filtering methods selected are appropriate, effective and reasonable.

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 unusual circumstances to call parents/ carer's emergency contact numbers directly.
- The sending of abusive text messages is forbidden.
- The school 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 / offfices / medical cabinet 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 computers; they must be down-loaded to the school system, then copied to disk 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.
- 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

- Generally speaking, school equipment must be used only for school business.
- Adults must have absolute control where a lap-top is taken home. It must only be used by the staff member to whom it is allocated and passwords must not be shared with anyone else.
- Staff members 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 down loading 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 1998.

4 Policy Decisions

4.1. Authorising access to the school system

- All staff and governors must read and sign the Acceptable Use Agreement (Staff Code of Conduct) before using any school ICT resource.
- The school 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 be allowed access to the school network at the discretion of the Senior Leadership Team.

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. Neither the school nor Warwickshire County Council can accept liability for the material accessed, or any consequences of Internet access.

- The Senior Leadership Team will audit ICT use to establish if the E-Safety Policy is adequate and that the implantation of the E-Safety Policy is appropriate and effective.

4.3. 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 and will follow the schools Behaviour Management Policy/sanctions.
- Young people and parents will be informed about any complaints procedures and the consequences for young people misusing the Internet.
- Any complaints about staff misuse must be referred to the Principal/senior leadership team.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

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.

5 Communications

5.1. Sharing the E-Safety Policy with 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.

5.2. Sharing the E-Safety Policy with staff

- All staff will have access to the School 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" 2016.
- The Education and Inspections Act 2006, provides statutory powers for staff to discipline Young people for inappropriate behaviour or for not following instructions, both on and off school premises; to confiscate items from young people as a disciplinary penalty. These powers 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 teachers the power 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.

- Ofsted judge the performance on a school in E-Safety.

7. Key Personnel

The Senior Leadership Team will act as the E-Safety Coordinators for the site.

The Designated Child Protection Lead Officers are:

- Matthew Pike - Principal
- Emily Bott, Chris Harlan-Marks, Shane Rowe – Assistant Principals
- Lorraine Nicholls – Safeguarding Lead
- Vikki Smith, Mary Doherty & Donna Mallabone