MacIntyre Academies

Endeavour Academy

Online Safety Policy

Version 7

Version	Purpose/Change		Responsibility	Date
V5	1 1 2.2 3.5 3.6	Updated to reference Keeping Children Safe In Education September 2020 Designated Safeguarding Officer details updated Nominated Safeguarding Lead LAB member email added Updated to reflect practice (students are taught to understand what is appropriate, as well as supervised) Clarification – use of staff mobile phones (restricted to breaks & specific locations) Clarification around when a student has a mobile phone they use for communication.	Principal	Jan 21
V6	1 1 Throughout	Updated to reference Keeping Children Safe in Education September 2021 Updated list of Safeguarding Leads and Officers Terminology change pupil – student	Principal	Mar 22
V7	Throughout	Change terminology – E-Safety to Online Safety Updated to reflect changes to statutory Guidance The Academy is signed up to the DfE Police Cyber Alarm	Principal	June 2023

Person Responsible: Principal
Type of Policy Non-statutory
Date of first draft: October 2015
Date of staff consultation: October 2015
Date approved by MAT Board: July 2016
Date of implementation: July 2016
Date reviewed: June 2023
Date of next review: June 2024

Contents

1. Introduction

This policy applies to both Endeavour School and Endeavour House, together these are referred to as Endeavour Academy, or the 'Academy'.

The policy must be read in conjunction with

- The latest version of Keeping Children Safe in Education (Being 2022 at the time of reviewing this policy)
- Oxfordshire Safeguarding Children Board's online safety information
- Preventing and tacking bullying, DfE, 2017
- Cyber bullying – advice for headteachers and school staff, DfE, 2014
- Education Act, 1996
- Teaching online safety in schools, DfE, 2023

In addition, this policy needs to be read in conjunction with the following Academy and Trust Policies:

- Endeavour Academy Safeguarding & Child Protection Policy
- Endeavour Academy Anti-Bullying Policy
- MacIntyre Academies Trust (MAT) Acceptable Use of Information and Communication Technologies (ICT)

Endeavour Academy recognises that the Internet, and access to it via a range of technologies, is an attractive and increasingly integral feature of student's learning and entertainment. The

Academy recognises too, that in enabling access to this invaluable resource it has a duty to ensure the students 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
- Safe from radicalisation
- Safe from grooming
- Secure, stable and cared for while online

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

This Policy document is drawn up to protect all parties – the students, the staff and the Academy, and aims to provide clear advice and guidance on how to minimise risks.

Research has proven that use of technology brings enormous 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 helps students to develop the skills and confidence to manage potential risks and considerably reduce their impact. It also ensures that staff members working at the Academy are aware of how to protect students against such risk, and to considerably reduce their impact.

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

2. Teaching and Learning

2.1 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 students with quality Internet access as part of their learning experience. Children with autism also find the use of computers, iPads, iPhones, Kindles and the internet highly motivating and a functional way to learn and communicate.

Post-Covid, virtual contact with families and external stakeholders has become a part of everyday life for our students.

ICT is used across the Academy, including at Endeavour House, 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 is also used for student's relaxation time and reward time within both the school and Endeavour House.

2.2 Internet use enhances learning

Internet browsing is enabled on iPads and Kindles and internet filtering is provided on all ICT

devices and can be disabled if and where needed. Students are also encouraged to use Apps instead i.e. YouTube kids.

The Academy's internet safety mechanisms ensure that students are protected against accessing content and information which is unsuitable, and deemed to be inappropriate for their age group. Appropriate filtering and monitoring systems are in place, which are updated on a regular basis and keep users safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. As some students are able to browse the internet independently extensive range of blocked keywords is applied to remove any adult content, as well as content linked to radicalisation and terrorism. This browsing is monitored by staff to ensure that students remain safe, rather than risk over blocking content.

Students are supervised and taught to understand what is and is not appropriate use of the internet.

Where appropriate, students are shown how to publish and present information to a wider audience using the internet as a tool.

The length of time students are online is monitored so this does not adversely affect their health and wellbeing.

2.3 Students are taught how to evaluate internet content

The Academy ensures that the use of internet derived materials by staff and students complies with copyright law.

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

Students are taught/encouraged to know:

- 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 (www.ceop.police.uk) 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.

3. Managing Information Systems

3.1 Information system security

Academy ICT systems' security is reviewed regularly. The system requires staff passwords to be updated regularly in accordance with the MAT Acceptable Use of ICT Policy, however student passwords might remain the same for a longer period of time.

Virus protection is updated regularly and assessed as appropriate for need. Any virus attacks are shared with the Group Director via our IT Support Company.
Security strategies will be discussed with the Local Authority and advice sought from the advisory services available from Oxfordshire County Council's Safeguarding Children Board.

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

Guests who would like to link to the internet whilst visiting the school site are permitted to do so through the Guest Wi-Fi log in, which is secure and does not give access to shared drives and folders which may contain sensitive information.

The Academy uses the Smoothwall 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 student) log in details. Line Managers hold any necessary meetings with staff members who may have accessed inappropriate content.

The Academy is signed up to Police Cyber Alarm, an initiative of the Department for Education to monitor threats received by the academy, in order to arrange appropriate mitigation measures.

3.2 E-mail

Staff and students may only use approved e-mail accounts on the Trust wide system which are assigned to them as individuals.

Confidential / sensitive information is sent encrypted using Egress Switch, as used by Oxfordshire County Council, to agencies outside of the Academy regarding students.

Staff ensure that in e-mail communication, students must not reveal their personal details or those of others, or to arrange to meet anyone without specific permission. All students are supported to use their email accounts appropriately.

The forwarding of chain letters is not permitted.

Office 365 Junk email filtering is in place. Incoming e-mail is treated as suspicious and attachments not opened unless the author is known.

The Academy monitors how e-mail from students to external bodies is presented and this is checked to ensure it is being sent to an appropriate receiver.

Staff support students when they are using email at all times. If any offensive emails are received or sent by a student, these are be noted and reported to a member of the Senior Leadership Team.

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

E-mail is one of the primary communication tools within the Academy and staff are expected to monitor their accounts regularly.

E-mails have the same legal status as written correspondence, and staff are responsible for using email safely and legally and, where appropriate, maintaining confidentiality.

Emails should not be considered as fully-secured medium. Users are responsible for ensuring correct addressing and appropriate content and taking special care when forwarding or replying to emails. Secure email system Egress must be used for communication with external stakeholders when any personal data is being used.

3.3 Published content and the Academy website

The contact details given on the website is the Academy address, e-mail and telephone number. Staff or student personal contact information is not published.

The Senior Leadership Team takes overall editorial responsibility and ensures that content is accurate and appropriate.

3.4 Publishing student's images and work

Written permission is sought from parents and carers before photographs of students are published on the Academy website/ social media.

A current list is kept to show the permissions given by parents for student's images to be published on the website/social media.

Students full names are not used anywhere on the Academy website, Twitter or any other forum, particularly in association with photographs.

Image file names do not refer to students by name.

Parents should be clearly informed of the Academy policy on image taking and publishing, both on Academy and independent electronic repositories.

3.5 Social networking, personal publishing and personal mobile devices

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

Social media sites are blocked through the Academy Wi-Fi.

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

Staff must not contact students, parents or family members on social networking sites.

Students and parents are advised that the use of social network spaces outside the Academy brings a range of dangers for students and that these are to be carefully monitored.

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

The use of personal mobile devices during school time is prohibited for all students unless otherwise agreed with the Senior Leadership Team. Should students need to use personal mobile devices this should be done in a safe location where images or video footage of others can't be obtained. Safe spaces such as locked cupboards are offered to students should they bring their device to school.

In Endeavour House students are allowed to use their personal mobile devices in the safe areas i.e. in their bedrooms or under supervision in communal areas. No images or video footage of others can be obtained on personal mobile devices.

The Academy will work with Social Care and families to make sure that devices which students use can be safely monitored through parental controls, should parents want advice on this.

Staff Personal mobile phones are not permitted to be used in the Academy when working with students. The academy provides a number of company phones in order to prevent use of personal devices. Staff personal mobile devices can be used only when a staff member is on the break and must be used in safe locations such as staffrooms or outside Endeavour Academy.

The use of cameras by students on mobile devices will be kept under review. Some students use their mobile device as their form of communication and photos might be on their system. All parties involved must consent to the use of any images. Staff are not permitted to use the cameras on their personal phone to take photos of students for any means.

3.6 Managing filtering

The Academy ensures systems to protect students are reviewed regularly and changed as required.

If staff or students come across unsuitable online materials, the site is reported to or other named Safeguarding Officer immediately. Should there be a need to report this further, then the appropriate advice will be sought.

3.7 Managing videoconferencing (Teams, Zoom) & webcam use

Videoconferencing is a big part of our day to day communication – internal and external. The use of webcams outside meeting rooms requires the permission of the Principal, the Head of Care or another member of the Senior Leadership Team. Webcams can be used in the meeting rooms only if all participants agree.

Webcams are used on central computers and laptops, of which all staff members are aware and under the login of senior members of staff or team leaders/teachers. These will not be permitted through the use of guest computers or laptops unless pre-agreed and risk assessed by the Principal or member of the Senior Leadership Team.

Skype/FaceTime

Webcams and the use of Skype/FaceTime is an important way for students to keep in contact with parents and families. Webcams used for Skype/FaceTime conversations are limited to specific devices. Access to the Skype account is limited to named members of staff. Access to FaceTime is monitored and staff members must support the exchange.

Staff members must ensure that they have checked the Skype/FaceTime link before students access this as a way of communicating with their families.

Parents are asked for permission to interact with their child in this way, and for their Skype/FaceTime contact to be shared with specific members of the staff team who will support students to use Skype/FaceTime as a form of contact.

No video recordings of students communicating with the families will be made.

3.8 Managing emerging technologies

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

Gaming machines, including Sony PlayStation and Microsoft Xbox, potentially have Internet access. Staff supervise students who access such devices and ensure that the internet access is not available.

iPads, iPhones, Kindles and smart speakers are continually monitored, and all wireless access for such devices is controlled through the Academy account and Guest account.

3.9 Protecting personal data

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 2018.
Breach of GDPR must be reported on the GDPRiS (GDPR in Schools) system in accordance with the MAT Data Protection Policy and the MAT Personal Data Breaches Procedures.

4. Policy Decisions

4.1 Authorising Internet Access

The Academy maintains a current record, through their IT support provider, of all staff and students who are granted access to Academy ICT systems and what their login details are.

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

4.2 Assessing risks

The Academy takes 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 Academy network. The Academy cannot accept liability for any material accessed, or any consequences of Internet access.

The Academy uses the OSCB audit tool to establish that the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

There is an Online Safety Risk Assessment in place which is updated on an annual basis.

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 student has seen.

Each student will have their own Risk Assessment for the use of the internet and devices which will detail the support required and possible risks to the student.

All staff are required to complete Online Safety training and Prevent training as part of the Safeguarding training.

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

4.3 Handling online 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 Academy Safeguarding and Child Protection Policy.

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

Complaints are logged and monitored by the Senior Leadership Team and information shared with appropriate agencies involved with individual students such as Social Care and LD CAMHS where a multiagency working approach is in place.

Advice around who to contact to make records of complaints will be sought in line with Safeguarding procedures at Oxfordshire Safeguarding Children's Board and Oxfordshire County Council.

http://www.oscb.org.uk/

5 Communications Policy

5.1 Introducing Online Safety Policy to students

Students are informed that network and internet use is monitored and appropriately followed up. Staff working with students are required to reinforce this through supervision and monitoring of students when they use the internet.

Online Safety work is delivered through relevant curriculum areas and pertinent and relevant information appropriate for the students' cognitive understanding is shared and taught.

Students have access to YouTube for Kids App, and some students are able to access YouTube through an internet browser. Students are supported to understand that some of the content of these sites is not available for their use, and will be blocked as in accordance with the own sites policies.

Personal mobile devices are not permitted during learning hours unless used as communication device. All personal mobile devices must be placed to a safe place (office, lock cabinet in the classroom etc.). In order to encourage positive and safe e-learning and giving students much needed life skills around ICT, GDPR, online safety and child protection students have access to Academy's wide range of ICT devices (iPhones, iPads, Desktop computers, Laptops, Smart speakers, Kindles etc.)

When student mobile devices are used for communication purposes additional safeguarding processes must be in place for such devices and students and parents must be aware that school will monitor the use as a part of the safeguarding procedures.

5.2 Staff and the Online Safety Policy

The Online Safety Policy is given to each staff member as part of their induction, and they have to read and sign to say they understand and agree with the policy.

Staff are informed that network and internet traffic can be monitored and traced to the individual user.

Staff understand what it means to be 'safe' on the internet, and in the context of children and young people with Autism accessing and using the internet.

All staff are expected to comply with the Online Policy at all times to protect the confidentiality and interests of the MAT and the Academy, employees, students, and the public.
Breach of this policy may lead to action under the MAT's Disciplinary Procedure.

5.3 Enlisting parents' and carers' support

Parents' and carers' attention is drawn to the Academy Online Safety Policy on the Academy website.

The Academy maintains a list of online safety resources for parents and carers and shares these as appropriate.

Links to further safety information is shared on the Academy website.

6 Resources

Appendix 1 lists resources of use for parents, carers, staff members and students.

Oxfordshire County Council: www.oxfordshire.gov.uk/cms/content/internet-safety-advice
Information and resources on internet safety

Oxfordshire Safeguarding Children Board e-Safety training: www.oscb.org.uk/e-safety
Free e-Safety courses

Oxfordshire Youth Website: www.oxme.info Guidance for young people

Child Exploitation and Online Protection Command: www.ceop.police.uk
Part of the National Crime Agency where reports of online abuse can be made. There is also a range of information for children, parents and professionals

Childnet International: www.childnet.com
Tips, resources and advice for young people, parents and teachers

Get Safe Online: www.getsafeonline.org Provides advice on using the internet securely

Internet Watch Foundation: www.iwf.org.uk
Provides a hotline to anonymously report online content which is child sex abuse; criminally obscene adult content; or non-photographic child sex abuse images.

NSPCC: www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware Advice for parents and a free helpline

South West Grid for Learning: www.swgfl.org.uk Provides resources, links and information on online safety

Think U Know: www.thinkuknow.co.uk
Provides online training and resources for parents, children and teachers

UK Safer Internet Centre: www.saferinternet.org.uk
Provides e-safety tips, advice and resources to help young people stay safe on the internet. It is a partnership of the charities Internet Watch Foundation, South West Grid for Learning and Childnet The centre also runs a helpline for all aspects of digital and online issues