Ormiston Endeavour Academy

Online Safety Policy

Policy Version Control

Policy prepared by:	Ormiston Endeavour Academy
Responsible committee:	Local Governing Body
Date approved and ratified:	10/10/17
Date for review:	10/10/18

Change Control

Date	Changes made	Agreed by	Authorised for use by	Date of review

Monitoring and Review (if applicable)

Contents

1.0 INTRODUCTION

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of Academy. It includes education for all members of the Academy community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Academies and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Academies must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good Online Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an Online Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, students and members of the wider Academy community. It is crucial that all are aware of the offline consequences that online actions can have.
Academies must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Principal and the Governing body.

The e-Safety policy is essential in setting out how the Academy plans to develop and establish its e- Safety approach and to identify core principles which all members of the Academy community need to be aware of and understand.

1.1 Links to Other Policies

The e-Safety Policy is linked to other Academy policies including:

- Acceptable use Policy
- Safeguarding Policy
- Anti-bullying
- Staff code of conduct

It should relate to other policies including those for:

- Behaviour;
- Personal, social and health education (PSHE);
- Citizenship.

2.0 TEACHING AND LEARNING

Why is Internet use Important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning; The Internet is a part of everyday 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;
- Students use the Internet widely outside the Academy and need to learn how to evaluate Internet information and to take care of their own safety and security;
- The purpose of Internet use in the Academy is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management functions;
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use Benefit Education?

- Benefits of using the Internet in education include:
- access to worldwide educational resources including museums and art galleries; inclusion in the National Education Network which connects all UK Academies; educational and cultural exchanges between students worldwide;
- vocational, social and leisure use in libraries, clubs and at home; access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of Academies, support services and professional associations; improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with SCC and DfE; access to learning wherever and whenever convenient.

How can Internet use Enhance Learning?

- the Academy's Internet access will be designed to enhance and extend education; students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- the Academies will ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law;
- access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students;
- staff should guide students to online activities that will support the learning outcomes planned for the students' age and ability;
- students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will students learn how to evaluate Internet content?

- students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
- students will use age-appropriate tools to research Internet content.
- staff will be aware of the need to keep students safe from terrorism and extremist material when accessing the internet and the school will ensure that suitable filtering is in place.

3.0 MANAGING INFORMATION SYSTEMS

How will information systems security be maintained?

- the security of the Academy information systems and users will be reviewed regularly; virus protection will be updated regularly;
- personal data sent over the Internet or taken off site will be encrypted;
- portable media may not be used without specific permission followed by an anti-virus / malware scan;
- unapproved software will not be allowed in work areas or attached to emails; files held on the Academy's network will be regularly checked;
- the ICT manager will review system capacity regularly;
- the use of user logins and passwords to access the Academy network will be enforced.

How will email be managed?

- students may only use approved email accounts for Academy purposes;
- students must immediately tell a designated member of staff if they receive offensive email; students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult;
- whole-class or group email addresses will be used in primary Academies for communication outside of the Academy;
- staff will only use official Academy provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team;
- access in the Academy to external personal email accounts may be blocked;

- emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper would be.
- the forwarding of chain messages is not permitted;
- staff should not use personal email accounts during Academy hours or for professional purposes.

How will published content be managed?

- the contact details on the website should be the Academy address, email and telephone number. Staff or students' personal information must not be published;
- email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT');
- the Vice Principal will take overall editorial responsibility for online content published by the Academy and will ensure that content published is accurate and appropriate;
- the Academy website will comply with the Academy's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can Students' images or work be published?

- images or videos that include students will be selected carefully and will not provide material that could be reused;
- students' full names will not be used anywhere on the website, particularly in association with photographs;
- written permission from parents or carers will be obtained before images/videos of students are electronically published;
- students work can only be published with their permission or the parents;
- written consent will be kept by the Academy where students' images are used for publicity purposes, until the image is no longer in use;
- the Academy will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will social networking, social media and personal publishing be managed?

- the Academy will control access to social media and social networking sites;
- students will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, Academy attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom;
- staff official blogs or wikis should be password protected and run from the Academy website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for Student use on a personal basis;
- personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the Academy where possible;
- students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private;
- all members of the Academy community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory; newsgroups will be blocked unless a specific use is approved;
- concerns regarding students' use of social networking, social media and personal publishing sites (in or out of Academy) will be raised with their parents/carers, particularly when concerning students' underage use of sites;
- staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Academy Acceptable Use Policy.

How will filtering be managed?

- the Academy's broadband access will include filtering appropriate to the age and maturity of students;
- the Academy will work with SCC and the Academies Broadband team to ensure that filtering policy is continually reviewed;

- the Academy will have a clear procedure for reporting breaches of filtering. All members of the Academy community (all staff and all students) will be aware of this procedure;
- if staff or students discover unsuitable sites, the URL will be reported to the Academy Network Manager who will then record the incident and escalate the concern as appropriate;
- the Academy filtering system will block all sites on the Internet Watch Foundation (IWF) list; changes to the Academy filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team;
- the Academy Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective;
- any material that the Academy believes is illegal will be reported to appropriate agencies such as Suffolk Police or CEOP;
- the Academy's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.

How will videoconferencing be managed?

- all videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer;
- equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name;
- external IP addresses will not be made available to other sites; videoconferencing contact information will not be put on the Academy Website; the equipment must be secure and if necessary locked away when not in use;
- academy videoconferencing equipment will not be taken off Academy premises without permission;
- responsibility for the use of the videoconferencing equipment outside Academy time will be established with care.

Users

- students will ask permission from a teacher before making or answering a videoconference call; videoconferencing will be supervised appropriately for the students' age and ability;
- parents and carers consent should be obtained prior to children taking part in videoconferences; only key administrators should be given access to videoconferencing administration areas or remote control pages;
- unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure;

Content

- when recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely;
- videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity;
- if third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights;
- establish dialogue with other conference participants before taking part in a videoconference. If it is a non-Academy site it is important to check that they are delivering material that is appropriate for your class.

How are emerging technologies managed?

- emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed;
- students will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the Academy Acceptable Use or Mobile Phone Policy.

How should personal data be protected?

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

4.0 POLICY DECISIONS

How will Internet access be authorised?

- the Academy will maintain a current record of all staff and Students who are granted access to the Academy's electronic communications;
- all staff will read and sign the 'Staff Information Systems Code of Conduct' or Academy Acceptable Use Policy before using any Academy ICT resources;
- parents will be asked to read the Academy Acceptable Use Policy for Student access and discuss it with their child, where appropriate;
- all visitors to the Academy site who require access to the Academies network or internet access will be asked to read and sign an Acceptable Use Policy;
- parents will be informed that students will be provided with supervised Internet access appropriate to their age and ability;
- when considering access for vulnerable members of the Academy community (such as with children with special education needs) the Academy will make decisions based on the specific needs and understanding of the student(s);
- secondary students will apply for Internet access individually by agreeing to comply with the Academy Online Safety Rules or Acceptable Use Policy.

How will risks be assessed?

- the Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via an Academy computer.
- Neither the Academy nor SCC can accept liability for the material accessed, or any consequences resulting from Internet use;
- the Academy will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the e–Safety policy is appropriate;
- the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Suffolk Police;
- methods to identify, assess and minimise risks will be reviewed regularly.

How will the Academy respond to any incidents of concern?

- all members of the Academy community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc);
- the e-Safety Coordinator will record all reported incidents and actions taken in the Academy Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log;
- the Designated Safeguarding Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately;
- the Academy will manage Online Safety incidents in accordance with the Academy discipline/ behaviour policy where appropriate;
- the Academy will inform parents/carers of any incidents of concerns as and when required. after any investigations are completed, the Academy will debrief, identify lessons learnt and implement any changes required;
- where there is cause for concern or fear that illegal activity has taken place or is taking place then the Academy will contact the Suffolk County Council Children's Safeguard Team or Online Safety officer and escalate the concern to the Police;
- if the Academy is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County Online Safety Officer;
- if an incident of concern needs to be passed beyond the Academy then the concern will be escalated to the Online Safety officer to communicate to other Academies in Suffolk.

How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the Academy's complaints procedure; Any complaints about staff misuse will be referred to the Principal;
- All Online Safety complaints and incidents will be recorded by the Academy, including any actions taken;
- Students and parents will be informed of the complaints procedure;
- Parents and students will need to work in partnership with the Academy to resolve issues;
- All members of the Academy community will need to be aware of the importance of confidentiality and the need to follow the official Academy procedures for reporting concerns;

- All members of the Academy community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the Academy community.

How is the Internet used across the community?

- the Academy will liaise with local organisations to establish a common approach to Online Safety; the Academy will be sensitive to Internet-related issues experienced by students out of Academy, e.g. social networking sites, and offer appropriate advice;
- the Academy will provide appropriate levels of supervision for students who use the internet and technology whilst on the Academy site;
- the Academy will provide an AUP for any guest who needs to access the Academy computer system or internet on site.

How will Cyberbullying be managed?

- cyberbullying (along with all other forms of bullying) of any member of the Academy community will not be tolerated. Full details are set out in the Academy's policy on anti-bullying and behaviour.
- there are clear procedures in place to support anyone in the Academy community affected by cyberbullying.
- all incidents of cyberbullying reported to the Academy will be recorded.
- there will be clear procedures in place to investigate incidents or allegations of Cyberbullying. students, staff and parents/carers will be advised to keep a record of the bullying as evidence. the Academy will take steps to identify the bully, where possible and appropriate. This may include examining Academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- students, staff and parents/carers will be required to work with the Academy to support the approach to cyberbullying and the Academy's Onlnie Safety ethos.
- sanctions for those involved in cyberbullying may include:
- the bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content;
- internet access may be suspended at Academy for the user for a period of time. Other sanctions for students and staff may also be used in accordance with the Academy's anti-bullying, behaviour policy or Acceptable Use Policy.
- parent/carers of students will be informed;
- the police will be contacted if a criminal offence is suspected.

How will Learning Platforms be managed?

- SLT and staff will regularly monitor the usage of the Learning Platforms by students and staff in all areas, in particular message and communication tools and publishing facilities;
- students/staff will be advised about acceptable conduct and use when using the Learning Platform;
- only members of the current student, parent/carers and staff community will have access to the Learning Platform;
- all users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platform;
- when staff, students etc leave the Academy their account or rights to specific Academy areas will be disabled or transferred to their new establishment.

How will mobile phones and personal devices be managed?

- the use of mobile phones and other personal devices by staff in Academy will be decided by the Academy and covered in the Academy Acceptable Use Policy;
- the sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Academy community and any breaches will be dealt with as part of the Academy discipline/behaviour policy;
- the use of mobile phones and personal devices by students are not permitted within the academy, if a mobile phone is seen by a member of staff it will confiscated and held in a secure place in the Academy office. Mobile phones and devices will be released to parents/carers.

Staff Use of Personal Devices

- staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- staff will be issued with an Academy phone where contact with students or parents/carers is required;

- mobile Phone and devices will be switched off or switched to ‘silent’ mode
- if members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team;
- staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose;
- if a member of staff breaches the Academy policy then disciplinary action may be taken.

5.0 COMMUNICATIONS POLICY

How will the policy be introduced to Students?

- all users will be informed that network and Internet use will be monitored;
- an Online Safety training programme will be established across the Academy to raise the awareness and importance of safe and responsible internet use amongst students;
- student instruction regarding responsible and safe use will precede Internet access.
- an Online Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe Academy and home use;
- Online Safety training will be part of the transition programme across the Key Stages and when moving between establishments;
- Online Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access;
- safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas;
- particular attention to Online Safety education will be given where Students are considered to be vulnerable.

How will the policy be discussed with staff?

- the Online Safety Policy will be formally provided to and discussed with all members of staff; to protect all staff and students, the Academy will implement Acceptable Use Policies;
- staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential;
- up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff;
- staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues;
- the Academy will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the students;
- all members of staff will be made aware that their online conduct out of Academy could have an impact on their role and reputation within Academy. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents’ support be enlisted?

- parents’ attention will be drawn to the Academy Online Safety Policy in newsletters, the Academy prospectus and on the Academy website;
- a partnership approach to Online Safety at home and at Academy with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days;
- parents will be encouraged to read the Academy Acceptable Use Policy for Students and discuss its implications with their children;
- information and guidance for parents on Online Safety will be made available to parents in a variety of formats;
- advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- interested parents will be referred to organisations listed in the “e–Safety Contacts and References section”.
- the Academy Online Safety Coordinator is Assistant Principal: Support for Learning.

What is good practice?

- awareness of the whole school community with opportunities for workshops for parents and students.
- robust reporting processes including use of peer mentors.
- annual staff training.
- policy regularly reviewed and updated.
- curriculum that engages students of all ages and teaches them how to stay safe and protect themselves and others.
- actively monitored filtering and use of a recognised internet service provider.
- monitoring and evaluation to assess the impact of e-safety practice.
- management of personal data in accordance with the Data Protection Act 1988.

Academy e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e- safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the Academy an e-Safety Policy that complies with Suffolk guidance?	Y/N
Date of latest update:	
Date of future review:	
The Academy e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. students, staff and parents/carers) consulted with when updating the Academy e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the Academies expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, students and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and USCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all students (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all Students?	Y/N
Do parents/carers or students sign an Acceptable Use Policy?	Y/N
Are staff, Students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the Academy filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N

Does the Academy log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the Academy e-Safety policy and ethos on a regular basis?	

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

e–Safety Officer, Children's Safeguards Team, Families and Social Care, Suffolk County Council. The e-Safety Officer is Rebecca Avery email: esafetyofficer@Suffolk.gov.uk
Tel: 01622 221469

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Suffolk County Council. The Children's Officer for Training & Development is Mike O'Connell email: mike.oconnell@Suffolk.gov.uk Tel: 01622 696677

Children's Safeguards Team: www.Suffolktrustweb.org.uk?safeguards

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EiS - ICT Support for Academies and ICT Security Advice: www.eisSuffolk.co.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Suffolk e–Safety in Academies Guidance: www.Suffolktrustweb.org.uk?esafety

Suffolk Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Suffolk Police via 01622 690690 or contact your Safer Academies Partnership Officer. Also visit www.Suffolk.police.uk or www.Suffolk.police.uk/internetsafety

Suffolk Public Service Network (KPSN): www.kpsn.net

Suffolk Safeguarding Children Board (KSCB): www.kscb.org.uk

Kidsmart: www.kidsmart.org.uk

Academies Broadband Service Desk - Help with filtering and network security: www.eisSuffolk.co.uk Tel: 01622 206040

Academies e–Safety Blog: www.Suffolktrustweb.org.uk?esafetyblog

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com