Ormiston Academies Trust

E-Safety Guidance Document

Authorised by

Name:	
Signed:	
Date:	

Issue Date:	
Review Date:	

Contents

Introduction

This document is provided to give outline guidance to academies when considering e-safety.

The provision for safety throughout the academy should not be limited to the contents of this document

What is e-safety?

E-safety may be described as an academies ability to protect and educate pupils and staff in the use of technology and the ability to identify threats; and to have appropriate mechanisms in place to support users in and the event of an incident.

The Ofsted guidance categories this into 3 areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm.

Requirements

E-safety is the collective responsibility of all members of staff taking on a shared and supportive approach to concerns, incidents and support.
The academy should;

- provide training for all staff (teaching and non-teaching). This should include but is not limited to:
  - Identifying risks.
  - Terminology and slang used.
  - Internal policy and procedures.
- ensure that the academy has implemented a clearly defined AUP (Acceptable Use Policy) and that all users have agreed to this.
- ensure that there is a clearly defined support, advice and reporting policies in place.
- offer outline advice and support to families of pupils. Including a mechanism for shared pupil support both when at home and in the academy.
- ensure that all staff are confident in offering basic support and advice to others.
- have regular reviews of new and emerging technologies and updating documents as appropriate.

E-safety is the collective responsibility of everyone. Engaging with families at all levels is key to ensuring that users are safe when using technology. Developing and maintaining relationships with families to support e-safety in the home.
Any discussions will need to include the opinions and views of the users. It has been identified that Pupils in the academies that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves

E-safety implementation Recommendations

This section is designed to offer advice on providing effective e-safety provision in an academy. To ensure that all applicable recommendations are followed we would recommend that the academy form an e-safety working group (this may be a sub section or agenda item of the ICT Working Group). Expectations of the working group will be covered in a later section.

Initial steps:

- Audit all staffs training needs. Design and structure a training plan to improve their knowledge of and expertise in the safe and appropriate use of new technologies.
- Review the current network service approach (Lockdown or managed) and guide support teams to change approach to a managed system and ensuring the academy provides a richer learning experience.
- Review / Create AUP for all users of the ICT systems. No user should be allowed access to ICT resource unless this has been agreed.
- Review current use of ICT both in the curriculum and during flexible access times.
- Review the current web access policies. (web filtering)[1]
- Review monitoring and logging services.[2]
- Review the academies data management policy for onsite and offsite date.

All steps should be regularly reviewed and changed as technology and its use evolve.

Moving forward:

- No personal data should leave the academies site without the appropriate encryption.
- No passwords for any account (administration, staff or student) should be shared with another user. Each user should have appropriate access assigned to their account. There should be a simple but effective user privilege and access request form for a user to improve their access rights as required.
- The academy requires policies covering the key areas for all aspects of academic life. These policies should be reviewed and updated as appropriate but with minimum review dates assigned.
- Educating users (staff and students) on safe use of ICT should be conducted and reviewed termly.
- All incoming internet access should be filtered to a minimum agreed level. A flexible approach can be adopted above that. (for example, 6th form users may have an elevated level)
- The academy needs to adopt a simple policy for pupils to report e-safety concerns to the appropriate staff. This policy needs to be shared to all users on a regular basis and tested to ensure all users are confident in its use.

E-Safety Working Group

The forming of an E-Safety Working Group is required to ensure that a shared approach to e-safety is adopted and to work as a review body ensuring that policy is appropriate and effective.

The group will be expected to:

- review and share experience, incidents and best practice.
- organise appropriate training for staff and to offer a selection of support paths for families and students. (training that offers certification from appropriate organisations is recommended)
- review training needs and available support (recommended this is done annually)
- evaluate incidents and offer support and guidance to others.
- review new technologies and the implications on policies.
- plan engagement events with external support partners and families.
- review policy's and agree required changes

[1] Web filtering usually works on 2 simple principals known as "White List" or "Black list". A white list blocks all content unless specifically allowed. A black list allows all content unless stated. A black list approach is the most common and is usually supported with content scanning which allows for words etc. to be blocked in addition to the black list

[2] All access to the internet should be logged against an individual user. Additional software can also be used to offer a more robust monitoring package. This software can monitor all of the device activity and obtain screen captures of any misuse.

Areas of Risk

Areas of risk include but not limited to:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- public sharing sites; YouTube, peer to pear file sharing, torrents.

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Key features of good and outstanding practice

All data in this section is recommended by Ofsted Section 5 guidance documents

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e-safety issues. High quality leadership and management make e-safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-Safety Mark). A high priority given to training in e-safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based online reporting processes that are clearly understood by the whole school, allowing the pupils to report issues to nominated staff, for example SHARP. Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. At least one staff member has accredited training, for example CEOP, EPICT.
Policies	Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors.

	The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The e-safety policy should incorporate an Acceptable Usage Policy that is signed by pupils and/or parents as well as all staff and respected by all.
Education	A progressive curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider or RBC together with age/maturity related filtering that is actively monitored.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-safety. Using data effectively to assess the impact of e-safety practice and how this informs strategy.
Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

Useful Acronyms

Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use http://www.digizen.org/glossary/.

In addition, the following terms used in this document are explained below

Age related filtering	Differentiated access to online content managed by the school and dependent on age and appropriate need (commonly used providers include Smoothwall, Lightspeed, Netsweeper, RM).
AUP	Acceptable Use Policy
Byron Review	Professor Tanya Byron's seminal report from 2008, 'Safer Children in a Digital World' available at http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.
CEOP	Child Exploitation and Online Protection centre.
Cyber bullying	Bullying using technology such as computers and mobile phones.
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
EPICT	European Pedagogical ICT Accreditation.
E-safety mark	Accreditation for schools reaching threshold levels within 360 degree safe through assessment by external assessor.
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, and Nintendo DS.
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
Impact level	Impact levels indicate the sensitivity of data and the associated protection required (see the government published HMG Security Policy Framework http://www.cabinetoffice.gov.uk/spf). The scheme uses five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification, however some (for example the home address of a child (or vulnerable adult) at risk) will be marked as RESTRICT.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).
Lifestyle website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Locked down system	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their

	teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed system	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as 'fishing' this is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen.
Profile	Personal information held by the user on a social networking site.
RBC	Regional Broadband Consortium, often providers of schools broadband internet connectivity and services in England, for example SWGfL, London Grid for Learning (LGfL).
Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SGII	Self-generated indecent images (often referred to as "sexting" –see above)
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process).
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people.
Spam	An e-mail message sent to a large number of people without their consent, usually promoting a product or service (also known as Unsolicited Commercial Email (UCE) or junk email).
Trojan	A malware program that is not what it seems to be. Trojan horses pretend to be useful programs like word processors but really install spyware or adware or open up a computer to hackers.
YouTube	Social networking site where users can upload, publish and share video.

Sample AUP Content

Before using the Internet it is imperative that all users agree to the academies Acceptable Use Policy. For students this will also require the parent or guardian to agree on behalf of the student. (note: this is in addition to the pupils agreement). This will make your students responsible for their actions and will educate your community about the guidelines you have established before you begin to use the Internet in instruction.

Below is an example of a parental consent form

ICT Usage Permission Form

Student Name:
Student Form:
Student Year:

Dear Parent or Guardian:
With your permission your child will be able to access the Internet at school as part of their class instruction. Below are the rules for Internet use at the school. Please read them over before you consider granting permission.

Guidelines for Internet Usage:

- All students must have a signed permission slip from their parent or guardian that authorizes them access to the Internet.
- Respect for the computer equipment and its network is a condition for use of the computers.
- Students are to notify the teacher/librarian immediately of any disturbing material they may encounter on the Web or in e-mail.
- For safety reasons, students are not to give out personal information such as telephone number, full name, address, etc. to anyone on the Internet.
- Students must never give anyone their password or allow another student to use their account to access the Internet or the school's network.
- Students must get permission from the teacher/librarian before downloading any programs from the Internet.
- If a student wants to use a floppy disk for the computer, it must be scanned for viruses by the teacher/librarian before being used.

Violation of any of these rules may result in forfeiture of permission to use the Internet and school network and/or appropriate disciplinary action. Please sign below if granting

Signed Declaration Section: This section will contain space for parental signature and date.

Computer Usage and Internet Policy

Internet access has been established for a limited educational purpose that shall be consistent with the schools' curriculum and the State Standards. The term "educational purpose" includes academic activities, career development, and approved limited, high-quality activities.
All students and parent/guardians must sign a copy of this policy and return it to their teacher prior to being allowed to use a computer.

- Under no circumstances should a student provide passwords to other students or allow anyone to use their login and password.

- Students are not authorized to load any software on a computer system.
- Students are not allowed to play CDs or DVDs on the school's computers.
- Students are restricted from using obscene, profane, lewd, vulgar, rude, threatening, or disrespectful language while using the school's computers.
- Students are not allowed to plagiarize works found on the Internet. Copy and pasting work from the Internet into your work is a form of plagiarizing.
- Students are restricted from changing the set-ups of the computers and removing or adding programs to any of the school's computers.
- There is no food or beverage allowed around the computers.
- Students may not unplug any keyboards or mice without prior permission from a teacher.
- Students are responsible to report any problems they see with the computers immediately to a teacher.

Acceptable uses of the Internet are activities which support learning and teaching.

Students must not:

- Violate the rights to privacy of other students.
- Use profanity, obscenity, or other language which may be offensive to another user.
- Copy materials in violation of copyright laws.
- Plagiarize.
- Reveal phone numbers, addresses or other personal information.
- Access, download, store, or print files or messages that are obscene or degrade others.
- Download or copy information on to floppy disks or hard drives without prior teacher approval

Failure to follow these rules and standards can result in the suspension of the student's computer account and/or other disciplinary action.

DECLERATION AND SIGNATURE

Student Computer and Internet Usage Agreement

We are very pleased to be able to offer Internet access to our students. The Internet offers vast, diverse, and unique resources from which everyone can benefit. Our goal as a school is to provide Internet service to promote educational excellence. All students that wish to use the school's computers and Internet must have a signed Student Computer and Internet Usage Agreement on file with their teacher.
With access to computers and people all over the world also comes the availability of material that might be undesirable or not of educational value. As a school, we have taken precautions to restrict access to many controversial materials by installing the Global Chalkboard, a filtering product developed by BASCOM.

Internet - Terms and Conditions

- Acceptable Use - The purpose of Internet access is to support research and education providing access to unique resources. The use of your account must be for educational purposes only.
- Privileges - The use of computers and the Internet is a privilege, not a right, and inappropriate use can result in a cancellation of those privileges.
- Network Etiquette - You are expected to follow the generally accepted rules of network etiquette. These include, but are not limited to, the following:
  - Do not make any changes to computer programs or setups on computers.
  - Use appropriate language.
  - Do not give out your or someone else's personal information such as last name, address or phone number.
- Security - Security on all computers is a high priority. If you feel you can identify a security problem on the school network, you must notify a teacher immediately. Do not use other users' individual accounts or share your password with anyone.
- Vandalism - Vandalism will result in a suspension of your computer privileges. Vandalism is any attempt to break a computer or to, intentionally upload a computer virus.

You do not have permission to install any software programs or download any programs from the Internet to the computers.

DECLERATION AND SIGNATURE