E Safety Guidelines

Scope: Eden Academy Schools

Category:	E-Safety Guidelines
Authorised By:	Board of Directors
Signature:	
Signed By:	Barry Nolan
Author:	Hilary McDermott
Version:	2
Status:	
Issue Date:	March 2nd 2017
Next Review Date:	March 2020

Contents

Eden Academy E-safety Guidelines

Pupil Use of the School's Internet and E-mail Services

DO

- Ensure that you are aware of the relevant internet and e-mail based skills that you are teaching the pupils

- Use focused search tasks rather than very open research tasks for pupils to ensure that accidental access to inappropriate web sites is reduced

- Use sites saved to favourites whenever possible to reduce accidental access to other sites

- Use sites known to be child safe whenever possible

- Check any open searches you intend to ask pupils to do in advance to ensure you are aware of the risks

- Ensure you know the procedure to follow if a pupil finds an unsafe site during lesson time. Switch off the monitor straight away but leave the computer on so that you can make a note of the web address. Report this to the Network Manager and Head straight away so that future access can be prevented.

- Teach pupils what to do if they accidentally find an unsafe site while using the Internet

- Teach pupils not to use any personal information such as name or address when e-mailing or using the Internet and the reasons why this could be unsafe

- Teach pupils that web sources could be unreliable and inaccurate and to check their information against other sources and not to rely on just one information source

- Always supervise pupil use of the internet and e-mail with pupils

- Ensure that internet use is monitored. The Network manager or Head will periodically check no users are visiting unsafe sites.

- Ensure parents are made aware of the risks of Internet and e-mail use in order that they can take precautions at home

- Be aware that searches for images may result in unsafe images as pictures are not easy to filter out. Test the search first and check not just the first page/s of returns to be sure.

- **DO NOT**

- Leave pupils to use the Internet unsupervised.

- Log pupils on to a personal account. Use class or pupil accounts for when pupils are working on a computer.

- **Staff Use of the School's Internet Service**

- E safety training will be delivered annually within school and as part of induction for all staff

- The school management wish to encourage the use of email and internet by staff in support of their work.

- Whilst staff are encouraged to use email and the internet in support of their work all use of these facilities should be appropriate to the work, standards and ethos of the school.

- The use of the school's internet and email systems are not provided as a right to any of their users. They may be withdrawn from any user adult or pupil who does not conform to the Eden Academy ICT Usage Policy

- The school is responsible for authorising any user of its internet or email facilities, monitoring and policing their use.

- Any member of staff who commits a serious offence in the use of the schools Internet service may be subject to the school's staff disciplinary procedures.

- Any user, adult or pupil, who breaks the law in respect of using the school's Internet service will be reported to the police.

- Personal use of the school's email system and internet is restricted to break times, lunchtimes and before and after school, and is at the discretion of the Head and the governing body.

- Staff or administrative users will make every effort to protect the school from computer virus attack or technical disruption

- Never pass on, or make obvious, or leave in an insecure place any passwords associated with using the Internet, email or computer system, including remote access

- Do not procure goods or services direct over the internet except by specific agreement with the Head.

- Never provide personal details or contact details of your own, or any other person, to Internet sites including weblogs, forums or chat rooms. Exceptions should be checked with your line manager or Head. At all times comply with the *Data Protection Act.*

- If you see any unacceptable site or material as a result of an innocent Internet query, unsolicited pop-up window or in any other way, report it immediately to the Network Manager and to the Head. Action can then be taken to block the site or material.

- Staff or approved adult school user should at all times abide by the *copyright laws* in respect of documents and materials downloaded from the Internet.

- Staff using a school Laptop or other device off the school site, at home or elsewhere or accessing the school's network through remote access, will still have to abide by the Eden Academy ICT Usage Policy. Colleagues will be aware that the misuse of such devices for activity not agreed by the school may be breaking the law under the *Computer Misuse Act 1990.*

- Never upload an image to a web site without complying with the academy and school's guidance on images loaded to the Internet.

- Staff will at all times work to maximise the safety of pupils within their care in their use of the Internet

- The school will maintain a record of all staff and pupils who are provided Internet access via the school's Internet service. This record will be kept up-to-date and be designed to handle common eventualities such as a member of staff leaving or a pupil's access be withdrawn etc.

- Colleagues will be aware of the ethos, standards, equalities and ethnic mix of the school and will not access any Internet material, or work with the Internet, in any way that infringes or offends these.

- Schools should have a system in place to ensure that any laptop computer being connected to its computer network is checked for computer viruses. This includes all laptops for teachers.

• Communication using technology

It is important to remember that when we communicate with children and young people we remember our professional role.

Communication between children and young people, by whatever method, should take place within clear and professional boundaries. This includes the wider use of technology such as mobile phones, text messages, social networking sites, emails, digital cameras, videos, web-cams and blogs.

A child/young person, for purposes of this document, is a person up to the age of 18.

Email or text communication between as adult and a child/young person outside of agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications made through internet sites.

This means that adults should:

- Not give their personal contact details to children or young people, including their mobile telephone number or personal email address.

- Only use equipment (e.g. mobile phone) provided by the organisation to communicate with children, making sure that parents have given permission for this form of communication to take place)

- Only make contact with children for professional reasons in accordance with any organisational policy.
- Not use the internet or web based communication channels to send personal messages to children/young people.
- Be aware of the sensitive nature of information that is put into the public domain (Facebook, Myspace etc) and be mindful at all times that they **must not** allow children, young people or any parent to be listed as "friends" and **must not** allow themselves to be listed as "friend" on their sites.
- not request or respond to any personal information from a child or young person, other than that which might be appropriate as part of your professional role.
- not discuss your school on social networking sites
- not mention in a negative manner, the school, nor pupils, parents, or colleagues
- absolutely refrain from commenting on incidents that occur or have occurred within the school

The following are offered as additional guidelines:

Think about your profile picture

Facebook will display your profile picture even when your information is set to private. It will also show some of your friends' profile pictures.

Think about what you are publishing

Although you may have set strict privacy controls, the information could still be shared by one of your 'friends'. It is sensible to think that, once published, the information is no longer private.

Talk to your friends and contacts

They should understand the need to keep your information private and not post inappropriate or potentially embarrassing comments, pictures or video on an open site.

Protect your image

Many sites now encourage you to name (tag) people that appear in uploaded photographs. These tags can be indexed and the original photographs displayed in search results. Even though you don't post pictures you may find that your friends do.

Web Filtering

It is the Head's responsibility, together with the network manager, to ensure that the level of web filtering on school equipment is set at an appropriately high level. All schools in the academy use Azteq for technical support and network management. The level of web filtering will be agreed with the Head at each school and the responsibility delegated so that it is applied and monitored by Azteq. Any changes to web filtering need to be agreed by the Head.