SteinerAcademyExeter

e-safety and e-communication policy

Introduction

e-safety is defined as being safe from risks to personal safety and well being when using all fixed and mobile devices that allow access to the internet as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones and gaming consoles such as Xbox, Playstation and Wii.
Safeguarding against these risks is not just an ICT responsibility, it is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

Acceptable Usage Policies (AUPs) set out guidance for the acceptable, safe and responsible use of on-line technologies. These are included below.

E-safety Lead. The Academy's `e-safety lead` is the Designated Safeguarding Officer, currently Jenny Salmon and Clive Staples.
The responsibilities of the e-Safety Lead include:

- Maintaining the AUPs;
- Ensuring that the academy's policies and procedures include aspects of e-safety;
- Working with the ICT provider to ensure that the `filtering` is in place and is set at the correct level for staff, children and young people;
- Reporting issues to the Principal;
- Ensuring that e-safety is included in staff induction and is part of staff training;
- Monitoring and evaluating incidents that occur to inform future safeguarding developments.

The internet is an essential element in 21st century life and ICT knowledge, now seen as an important life-skill, is vital to access life-long learning and employment. It is also important to recognise that the internet provides many benefits. While acknowledging the benefits, it is also important to recognise that risk to safety and well-being of users is ever-changing as technologies develop. These can be summarised as follows:

• Content
  Commercial (adverts, spam, sponsorship, personal information)
  Aggressive (violent/hateful content)
  Sexual (pornographic or unwelcome sexual content)
  Values (bias, racism, misleading info or advice)

• Contact
  Commercial (tracking, harvesting personal information
  Aggressive (being bullied, harassed or stalked)
  Sexual (meeting strangers, being groomed)
  Values (self-harm, unwelcome persuasions)

• Conduct
  Commercial (illegal downloading, hacking, gambling, financial scams,terrorism)
  Aggressive (bullying or harassing another)
  Sexual (creating and uploading inappropriate material)
  Values (providing misleading info or advice)

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism that would be considered ***inappropriate and restricted*** elsewhere.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as ***'grooming'*** and may take place over a period of months using chat rooms, social networking sites and mobile phones.

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

Managing Incidents

- **Has there been inappropriate contact?**

1.Report to the organisation manager/e-safety lead/child protection officer
2.Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence
3.Contact the parent(s)/carer(s)
4.Contact the police on 101
5.Log the incident
6.Identify support for the child, young person or vulnerable adult

- **Has someone been bullied?**

1.Report to the organisation manager/e-safety lead/child protection officer
2.Advise the child, young person or vulnerable adult not to respond to the message
3.Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
4.Secure and preserve any evidence
5.Contact the parent(s)/carer(s)
6.Consider informing the police on 101, depending on the severity or repetitious nature of the offence
7.Log the incident
8.Identify support for the child, young person or vulnerable adult

- **Has someone made malicious/threatening comments?**

1.Report to the e-safety lead;
2.Secure and preserve any evidence
3.In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
4.Inform and request that the comments are removed from the site/block the sender
5.Inform the police on 101 as appropriate
6.Log the incident
7.Identify support for the child, young person or member of staff.

- **Has an inappropriate/illegal website been viewed?**

1.Report to the organisation manager/e-safety lead/child protection officer
2.If illegal (See Appendix F), do not log off the computer but disconnect from the electricity supply and contact the police on 101
3.Record the website address as well as the date and time of access
4.If inappropriate (See Appendix F), refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5.Decide on the appropriate sanction
6.Inform the parent(s)/carer(s)
7.Contact the filtering software provider to notify them of the website
8.Log the incident

e.safety rules for young pupils

- Ask permission before using the internet;
- Tell a trusted adult if you see anything that makes you feel uncomfortable;
- Immediately close any web-page that you are uncomfortable with;
- Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details;
- Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos;
- Only contact people that you have actually met in the real world;
- Never arrange to meet someone that you have only met on the internet;
- Only use a web-cam with people you know;
- Think very carefully about any pictures that you post online;
- Never be mean or nasty to anyone on the internet or when using a mobile phone. If you know of someone being mean to another person, tell a trusted adult;
- Only open e-mails from people that you know;
- Avoid using websites that you wouldn't tell anyone about and use a student friendly search engine such as http://www.askforkids.com .

Staff and Volunteers Agreement

I will familiarize myself with the Staff Employment Handbook's statements in the section `Communications`.

I will only use the Academy's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.

I will only use secure e-mail system(s) for any Academy business (web mail accounts are not secure e-mail system(s)).

I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.

I will report any accidental access, receipt of inappropriate materials or filtering breaches to the Principal or member of the management team.

I will not allow unauthorised individuals to access e-mail / internet / intranet / networks or systems.

I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself.

I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.

I will follow the DFE 2009 'Guidance for Safer Working Practice for Adults who work with Children and Young People' (http://www.timeplan.com/uploads/documents/Downloads/Safer-Working-Practices.pdf

I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.

I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.

I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.

I understand that all internet and network usage can be logged and this information could be made available to the Principal or management team on request.

I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum security specification.

I will not use personal digital cameras or camera phones for transferring images of children and young people or staff without permission.

I will not engage in any online activity that may compromise my professional responsibilities.

I understand that the Data Protection Act requires that any information seen by me with regard to staff or children and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

I will at all times behave responsibly and professionally in the digital world and will not publish any work-related content on the internet.

I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.

I understand that failure to comply with this Acceptable Use Policy (AUP) could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the Academy's most recent Acceptable Use Policy (AUP).

I agree to abide by the organisation’s most recent Acceptable Use Policy (AUP).

Signature …….…….…… Date ……Full Name

…….. (print)Job

title.....

Authorised Signature/Manager

I approve this user to be set-up.

Signature …….…….….. Date …… Full Name

…….…….. (print)

Cyberbullying/Inappropriate Behaviour on Facebook

1. If you know the identity of the perpetrator, contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed, often works.
2. Failing that, having kept a copy of the page or message in question, delete the content.
3. For messages, the 'delete and report / block user facilities' are found in the 'Actions' dropdown on the page on which the message appears.
4. For whole pages, the 'unfriend and report / block user facilities' are at the bottom of the left hand column. Always try to cite which of the Facebook Terms and Conditions have been violated (see note 10 for the most likely ones) at http://www.facebook.com/terms.php or Community Standards at http://www.facebook.com/communitystandards/. Note that Facebook are more alert to US law than UK. The process should be anonymous.
5. If the page is by someone under 13 click on http://www.facebook.com/help/contact.php?show_form=underage (Facebook say they will delete any such page).
6. To remove a post from a profile, hover over it and on the right there will be a cross to delete it.
7. Does the incident trigger the need to inform the police or child protection agencies?
8. To report abuse or harassment, email abuse@facebook.com (Facebook will acknowledge receipt of you email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint).
9. If all else fails, support the victim, if they wish, to click the 'Click CEOP' button http://www.thinkuknow.co.uk/
10. If the victim is determined to continue using Facebook, they might want to delete their account and start again under a different name. Deletion can be done here https://ssl.facebook.com/help/contact.php?show_form=delete_account. They should be made aware of the privacy issues that might have given rise to their problem in the first place:

    You will not bully, intimidate, or harass any user (1.3.6)

    You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission (4.1)

    You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law (5.1)

Parents and Carers Agreement

Internet and ICT: As the parent or legal guardian of the student(s) named below, I am aware that my *daughter / son* will have access to:

o the internet at school
o the school's chosen e-mail system
o the school's online managed learning environment
o ICT facilities and equipment at the school

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies but I understand that the school takes every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the internet sites they visit at school and, if there are concerns about my child's e-safety or behaviour online, they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The Use of Digital Images and Video" and I support this.

I understand that the school will necessarily use photographs of my child or include them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school and for no other purpose.

I will not take, and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on *"The Use of Social Networking and On-line Media."*

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the internet and digital technology at home. I will inform the school if I have any concerns.

I acknowledge that schools now have powers under the Education Act 2011 to search students for 'prohibited items' which covers any article that a member of staff suspects has been, or could be, used to commit an offence. These powers also allow the item to be seized, delivered to the police, returned to its owner, retained or disposed.

My daughter / son name(s): _____Parent / guardian signature: _____Date: ___/___/___

The Use of Digital Images and Video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter/son.

We follow these rules for any external use of digital images:

If the student is named, we avoid using their photograph.

If their photograph is used, we avoid naming the student.

Where showcasing examples of students' work, we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that students are not referred to by name on the video, and that students' full names are not given in credits at the end of the film.

Only images of students in suitable dress are used.
Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

Your child's image being used for presentation purposes around the school

e.g. in class or wider school wall displays or PowerPoint presentations.

(The school should make a judgement with the inclusion of the following statement):

- *Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.*

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission e.g. if your child won a national competition and wanted to be named in local or government literature.

The Use of Social Networking and On-Line Media

This school asks its whole community to promote the 3 'common' approaches to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- *We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.*

How do we show common decency online?

- We do not post comments that can be considered **intimidating, racist, sexist, homophobic or defamatory.** This is **cyber-bullying** and may be harassment or libel (i.e. a criminal act).
- When such comments exist online, we do not forward such emails, tweets, videos, etc. to other people/groups. This could be considered criminal behaviour.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, we check where it is saved and we check our privacy settings.
- We make sure we understand changes in any websites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social networking sites, this will be addressed by the school in the first instance. However, if necessary, the police may be involved and/or legal action pursued.

The school operates its own Facebook page for PR purposes. It does not support the use of additional Facebook pages set up by parents, staff or pupils which name the school, unless by prior agreement. Such agreement may be given where there are clear terms of reference, shared `management` and a recognised need, for example to promote an event or meeting.

Electronic Devices -Searching & Deleting

Introduction

All schools have a power to search for and seize items banned under school rules and also to delete data stored on seized electronic devices where there is `good reason`, i.e. where staff suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.

Items banned under the school rules are listed below and in the Parents' Handbook:
radios, tape players, electronic games, MP3 players, iPods or other portable music devices, cameras.
Mobile phones are only permitted where parents require children to confirm school journeys and transport arrangements. They should be kept turned off during the school day, including breaks.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.
DfE advice on these sections of the Education Act 2011 can be found in the document:
"Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

Search:

Pupils are allowed to bring mobile phones or other personal electronic devices to school and use them **only** within the rules laid down by the school.

If pupils breach these roles sanctions will be in line with those used for other breaches of school rules, including detention, exclusion or the setting up of an Individual Behaviour Programme.

Staff have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

Searching with consent: Authorised staff may search with the pupil's consent for any item.

Searching without consent: Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.

The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil.

Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where there appears to be a risk of serious harm unless the search is

carried out immediately.

Extent of the search:

The person conducting the search may not require the pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the pupil has or appears to have control – this includes desks, lockers and bags.

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it

requires the involvement of the police. (It is recommended that members of staff should know who to contact, within school, for further guidance before taking action and that the person or persons is or are named within this policy).

A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommend that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review e-safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Audit / Monitoring / Reporting / Review

The Designated Protection Officer will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

Further Guidance

CEOP (Child Exploitation and Online Protection Centre)
http://www.ceop.gov.uk

The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. That means that they are part of UK policing and very much about tracking and bringing offenders to account either directly or in partnership with local and international forces.

Think U Know
http://www.thinkuknow.co.uk

Think U Know is CEOP's support, guidance and resource site for children, young people, parents, carers and adults who work with children and young people.

UK Safer Internet Centre
http://www.saferinternet.org.uk/

This website provides the latest advice on how to use the internet and new technologies safely and responsibly. Also find a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies.

Childnet
http://www.childnet-int.org

Childnet is a non-profit organisation working with others to "help make the Internet a great and safe place for children". The website gives news and background to Childnet's work and serves as a portal to Childnet's award-winning projects.