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.

This policy along with the Parent/ Carer ICT Acceptable Usage Policy (AUP) (in Appendix) **and Steiner Academy Bristol's Staff Code of Conduct Policy** https://classroom.google.com/c/ODA4NTU4MTQ0Nlpa/mc/OTY2NjI0MTE0M1pa/details sets out guidance for the acceptable, safe and responsible use of on-line technologies.

E-safety Lead. The lead responsibility for e-safety falls to the academy's Safeguarding Team. The e-safety responsibilities 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 the 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. For example, there is information on weapons, crime and racism that would be considered ***inappropriate and restricted***. In addition, the school has a duty to prevent children from being drawn in to terrorism and other extremist movements.

All staff are expected to complete the Home Office's online Prevent training: https://www.elearning.prevent.homeoffice.gov.uk. This training helps equip staff identify children at risk. However, there is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. Radicalisation can occur quickly or over a long period. For further information or to report a concern please use the Police PREVENT Telephone number: 0117 9455539. Alternatively, contact a member of the Safeguarding team. For further details please refer to Steiner Academy Bristol's Safeguarding and Child Protection Policy: http://steineracademybristol.org.uk/files/8415/2664/4616/Safeguarding_and_Child_Protection_Policy_SAB_Approved_1804.pdf

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

Inappropriate Contact:

1. Report to the DSL/Safeguarding team
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 on CPOMS
6. Identify support for the child, young person or vulnerable adult

Online Bullying:

1. Report to the DSL/Safeguarding team
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 on CPOMS
8. Identify support for the child, young person or vulnerable adult

Malicious/threatening comments:

1. Report to the DSL/Safeguarding team;
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 on CPOMS
7. Identify support for the child, young person or member of staff.

Accessing inappropriate/illegal websites:

1. Report to the DSL/Safeguarding Team
2. If illegal 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 refer the child/young person 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 on CPOMS

E-safety rules and guidance for all pupils

In the Steiner Curriculum, there is no definitive age expectation regarding the use of Information Technology and Computers. However, it is crucial that staff assess the contextual intent before choosing to use technology and/or computers. For example, if students are collating and analysing weather data (for a Science project), then using spreadsheet software becomes contextualized, as it is an effective and efficient data management tool.

All students across the lower/middle and upper school will have the opportunity to explore e-safety in an age appropriate way via SAB's PSHE curriculum.

Pupil Online Rules and Etiquette

- 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 outside of school, 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 in the real world;
- Think very carefully about any pictures that you post online and know that posting explicit pictures is illegal;
- 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

All staff and volunteers must familiarise themselves with Steiner Academy Bristol's Staff Code of Conduct paying particular attention to the E-safety/ Communications section. Staff and Volunteers must sign the Staff Information Systems Declaration.

This includes:

- Protocol and Expectation
- Monitoring and Recording
- E-Communication and the Law
- Communication of the Policy
- Good Practice Guidance
- Email
- Social Media/Conduct
- Privacy & Privacy Settings
- Staff Information Systems Declaration

Cyberbullying/Inappropriate Behaviour on Facebook and other Social Media Sites.

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.

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 https://www.facebook.com/terms.php or Community Standards at https://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 https://en-gb.facebook.com/help/contact/209046679279097 (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 your email and start looking into your complaint within 24 hours).

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.
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)

The Use of Digital Images and Video

To comply with the Data Protection Act 2018 (GDPR), we need your permission before we can photograph or make recordings of your child.

All parents will receive a separate Acceptable Use of Photographing and Sharing Images upon Student admission.

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.

Staff 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 kindergarten 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.

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 libelous (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 libelous 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

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 and stored in the school office.

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"
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf

Search:

Pupils are advised not to bring mobile phones or other personal electronic devices to school. Steiner Academy Bristol are not liable for loss, damage or theft of said items.

Excluding emergencies, pupils are not permitted to use their mobile phones or other personal electronic devices on campus. Students with additional needs e.g. attachment disorders, may have an acceptable user agreement put in place, however this would need to be agreed by a member of the school's Leadership Team.

If pupils breach these roles consequences will be in line with those used for other breaches of school rules, including, use of the Rainbow Room for reflection and calming, internal exclusion, external exclusion and/or the setting up of an Individual Behaviour Agreement. In addition, all members of staff have the authority to confiscate pupil mobile phones and/or other electronic devices. Staff must stow the pupil's item in a safe place out of reach of other pupils and visitors. Where possible, staff should take said items to a member of the Leadership Team where it can be locked away. Steiner Academy Bristol reserve the right to request parental collection of mobile phones and/or other electronic devices.

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: Members of the Leadership Team may search with the pupil's consent for any item.

Searching without consent: Members of the Leadership Team 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:

Members of the Leadership Team 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 member of the Leadership Team 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.

Members of the school's Leadership Team 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.

All searches must be recorded on CPOMS providing full details of the incident including why a pupil search was necessary.

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 & Deletion of Data

A 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 Leadership Team/Safeguarding Team 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

Following an examination of an electronic device, if the 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 Leadership Team/Safeguarding Team 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, however 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). Any unlawful and/or inappropriate behavior involving electronic devices / data storage / internet usage should be recorded on the academy's safeguarding CPOMS system (MIS) and where appropriate/necessary police involvement. Where the above behaviors involve a member of academy staff the Principal may contact the police and LADO (Local Authority Designated Officer).

Audit / Monitoring / Reporting / Review

The Academy's Designated Safeguarding Lead 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)

https://www.ceop.police.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

https://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

https://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 focusing on the safe and responsible use of the internet and new technologies.

Childnet

https://www.childnet.com/

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.

Related Policies & Staff

- Staff Code of Conduct
- Safeguarding & Child Protection,
- Sex and Relationships Education
- Staff Code of Conduct
- Whistle Blowing

Leadership Team

- Joss Hayes – Principal/DSL
- Sophie Barlow- SENCo / DSL
- Richard Crossley- DSL Safeguarding & Welfare Lead
- Kamar Finn – Upper School Lead
- Emilie Graham – Maths Lead
- Rhiannon Kithen – English Lead/Pupil Premium

Document Control

Designated Governor (role)	Laura Watson (Safeguarding)
Designated Staff member	Richard Crossley
Governor Committee	TLC
Date Approved by Governors	July 2018
Review Date	July 2019

Appendix

Parents and Carers Acceptable Usage Policy

Internet and ICT: As the parent or legal guardian of the student(s) named below, I am aware

that my child will have access to:

- the internet at school
- the school's chosen e-mail system
- the school's online managed learning environment of 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 Acceptable use of Photographs and Sharing Images Policy and I support this.

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

I will not take photographs of other children (or staff) at school events without their express permission and I will not share photographs of other children/ staff.

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 child's name: _____

Parent / guardian signature: _____

Date: ___/___/___