Online Safety Policy

Document number:	**5**
Review frequency:	**Annually**
Last reviewed:	**December 2018**
Agreed by Governors	**21/1/19**
Next review date:	**December 2019**

Online Safety

At Trevithick Learning Academy we value the diversity of backgrounds of all pupils, families and wider school community.
We promote the fundamental British values of; democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs.
Our school reflects British values in all that we do. We aim to nurture our children on their journey through life so they can grow into safe, caring, democratic, responsible and tolerant adults who make a positive difference to British society and to the world. We encourage our children to be creative, unique, open-minded and independent individuals, respectful of themselves and of others in our school, our local community and the wider world.

Introduction

1.1. Online Safety encompasses Internet technologies and electronic communications such as mobile technology and wireless technology. Most young people are enthusiastic Internet users - particularly of interactive services like: Chat, gaming, vlogging and streaming via apps. However, like many exciting activities, there are risky situations to deal with and hazards to avoid.

1.2. Current and emerging technologies used in the Academy and, more importantly in many cases, used outside of the Academy by children include:

- The internet;
- Instant messaging (via Social Networking apps e.g. Instagram) using simple web cams and email;
- Blogs /vlogs (an on-line interactive diary);
- Streaming of video, radio, music (e.g YouTube);
- Social networking sites (e.g. www.facebook.com, www.instagram.com , www.whatsapp.com, www.snapchat.com);
- Gaming Sites (e.g. Roblox, Fortnite, Minecraft) and games consoles (e.g. Nintendo Switch, Xbox One and Playstation 4);
- Music and video download sites;
- Mobile technology (e.g. Smartphones, Tablets and wearables) with camera and video functionality;

1.3. The Primary Curriculum states that children should be responsible, competent, confident and creative users of information and communication technology.

KS1 Attainment Targets:

Use technology safely and respectfully, keeping personal information private: identify where to go for help and support when they have concerns about content or contact on the internet and other online technologies.

KS2 Attainment Targets:

Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

1.4. Across all areas of learning children:

- Find and select information from digital and online sources, making judgments about accuracy and reliability;
- Create, manipulate and process information using technology to capture and organise data, in order to investigate patterns and trends;
- Explore options using models and simulations; and combine still and moving images, sounds and text to create multimedia products;
- Collaborate, communicate and share information using connectivity to work with, and present to, people and audiences within and beyond the Academy;
- Refine and improve their work, making full use of the nature and pliability of digital information to explore options and improve outcomes.

Policies and Procedures

1.5. The Academy's Online Safety policy will operate in conjunction with other policies including: Password Security, Acceptable Use Agreements, Behaviour, Anti-Bullying, Teaching and Learning and Data Protection.

1.6. Our Online Safety Policy has been written building on SWGfL guidance.

1.7. The Online Safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.

1.8. All Academy pupils, staff and guests are to sign an Acceptable Use Agreement (AUA) detailing the ways that all network users should use our ICT facilities and reflects the need to raise awareness of the safety issues associated with electronic communications, access may be withheld if the relevant policy hasn't been completed. Regular guests may be supplied with a log in to network resources if required.

1.9. Online Safety will form a key part of the Computing & PSHE Curriculum. The school uses the SWGfL Digital Literacy resources. Children will be made aware of the dangers and risks of using the Internet and mobile technologies throughout the Academy year. This will include during anti-bullying week, Safer Internet Day and an integral part of Computing lessons.

Internet Access

1.10. The Internet is an essential element of education, business and social interaction. The Academy has a duty to provide pupils with quality Internet access as part of their learning experience.

1.11. Internet use is a part of our curriculum and a necessary tool for staff and pupils.

1.12. The Academy Internet access will be designed expressly for school use and will use appropriate filtering system, differentiating for relevant groups.

1.13. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will not use the Internet without having permission from a member of staff.

1.14. Pupils will not use social networking sites in the Academy and will be educated about their safe usage in their own time.

1.15. Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location.

1.16. Pupils are forbidden from downloading games or other programs from the Internet whilst in school.

1.17. The Network Manager or ICT TA will carry out downloading programs from the Internet.

1.18. Pupils will be educated in Digital Literacy and taught how to evaluate the Internet content that they have located. Pupils will be taught the importance of cross checking information before accepting its accuracy.

1.19. The Academy will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.

1.20. Pupils will be advised not to share any inappropriate content they receive and report it accordingly.

1.21. Pupils will be taught how to report unpleasant Internet content they are subjected to or made aware of.

1.22. Pupils will be advised never to take inappropriate images of themselves or others and then post, publish or share these images.

Messaging

1.23. When available, pupils may only use approved Academy Gmail accounts on the Academy network. Pupils are not permitted to use their own personal messaging accounts on Academy equipment.

1.24. Pupils must immediately tell a teacher if they receive an offensive message.

1.25. In communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

1.26. Incoming messages should be treated as suspicious and attachments/hyperlinks not opened unless the author is known.

1.27. Messages sent to any recipient should be written in a professional manner as all written correspondence is a representation of the academy.

1.28. The Network Manager or ICT TA will provide an official school email address. Staff should never use personal messaging addresses to communicate with pupils and only use Academy messaging addresses to communicate with pupils about pupil work.

1.29. Staff should only use Academy Gmail accounts for academy business and never send any academy information on personal messaging addresses.

Managed Learning Environment (Google Apps)

1.30. The Managed Learning Environment (MLE) is provided for use of The Academy staff, pupils and governors .

1.31. Pupils should never reveal their passwords to anyone or attempt to access the service using another pupil's login details. Pupils should inform the Network Manager/ ICT TA if they feel their password has been compromised.

1.32. All users possess a username and password as a level of security. The correct levels of privilege are applied to the correct users.

Published Content and the Academy Website

1.33. Staff or pupil's personal contact information will not be published. The contact details given online should be the Academy office.

1.34. The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.35. Permission from parents or carers will be obtained before photographs of pupils are published online. Pupils' full names will not be used anywhere on the web site or social media, particularly in association with photographs.

1.36. Pupil image file names will not refer to the pupil by name.

1.37. Pupil image files should only be securely stored on the Academy network or encrypted devices.

Video Conferencing and Webcam Use

1.38. When available, video conferencing and webcam use will be appropriately supervised.

1.39. Pupils will be taught the dangers of using photographic devices outside of the Academy.

Portable Equipment

1.40. The school does not permit the use of personal devices for Academy work or allow the connection to academy resources. Devices will be supplied by the network manager or ICT TA when required.

1.41. Mobile phones are not to be used in the Academy; for children who walk home alone then they are to be held securely in the classroom until the end of the day. The sending of abusive or inappropriate text messages is forbidden.

1.42. Staff and pupils should be aware of the mobile phone policy and adhere to it.

1.43. Staff should be aware that technologies such as tablets, wearables and mobile phones may access the Internet by bypassing filtering systems and present a new route to undesirable material and communications.

1.44. The use of wearables within the school premises is forbidden as they can present a security risk. Examples include, wearables which have the capacity to take photographic images. Wearables are therefore included in the mobile phone policy and must be treated accordingly.

1.45. Staff should not use their personal equipment to contact pupils or capture photographs of children. Alternative equipment will be provided by the Academy.

1.46. Pupils are taught how to protect themselves from being victims of theft and how to report such an event to the correct authority.

Managing Emerging Technologies

1.47. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.

Protecting Personal Data

1.48. Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) 2018.

1.49. All Academy portable devices are encrypted. Either with software or hardware encryption.

Roles and Responsibilities

1.50. The DSL is Will Johnson and the Safeguarding Governor is Andrew Mercer.

1.51. Support will be provided by the Network Manager and his team. Our Network Manager ensures they keep up to date with Online Safety issues and guidance; keeps the Principal, senior management and Governors updated as necessary; ensures that any Online Safety concerns are reported in the first instance to the DSL who will investigate the concern and take the appropriate action.

1.52. Our Governors have an understanding of Online Safety issues and strategies at the Academy, and are aware of local and national guidance on Online Safety and are updated at least annually on policy developments.

1.53. All our staff have Online Safety responsibilities: to be familiar with the policy and to adhere to its' procedures and must be familiar with the Academy's Policy in regard to:

- Safe use of e-mail;
- Safe use of internet;
- Safe use of the school network, equipment and data;

- Safe use of digital images and digital technologies, such as mobile phones, digital cameras, tablets and iPads;
- Publication of pupil information/photographs and use of the web site;
- Cyber bullying;
- Their role in providing Online Safety education for pupils;
- Staff should be aware that Internet traffic will be monitored and traced to the individual user. Discretion and professional conduct is essential;
- Staff will always use a child friendly, safe search engine when accessing the Internet with pupils. (e.g. Google Safe Search – default settings).

1.54. Academy staff will be reminded/updated about Online Safety matters at least once a year.

Managing Internet Access and Other Technologies

1.55. **Information system security**

1.55.1. Academy ICT systems capacity and security will be reviewed regularly.

1.55.2. All staff and pupils possess appropriate access rights and privileges inline with our Password Security Policy.

1.55.3. Virus protection will be installed on all Academy computers and updated regularly in light of new viruses and unwanted programs.

1.55.4. Staff must ask permission from the Network Manager before installing software on any Academy machines, which should normally be installed by the Network Manager.

1.55.5. External storage devices (hard drives, USB Sticks, Flash drives, etc.) should not be used. If one is required an encrypted drive can be obtained from the Network Manager.

1.56. **Managing filtering -**

1.56.1. If staff or pupils discover an unsuitable web site, it must be reported to the Network Manager or ICT TA, the screen can be closed but the computer should not be shut down to allow further investigation.

1.56.2. The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.56.3. The school uses a Lightspeed Rocket filter for its internet filtering. This uses Captive Portal to request user data before assigning filtering policies. Policies are also assigned through ip ranges. Staff and pupils have separate policies. Any visitor to the school will firstly receive the pupil policy. If anyone requires a higher level of access, it must first be approved by the Network Manager.

1.56.4. Our filter is Prevent Duty compliant, documented on https://www.lightspeedsystems.com/en-uk/prevent-duty/

> "*Lightspeed Systems Web Filter contains billions of URL's all arranged into education-focused categories. Most categories can be allowed or*

*blocked by admins to ensure schools have granular control over the content students can see. However, there are a number of sealed categories that are permanently blocked when it is determined that they have no educational value and may be potentially harmful to users, these sealed categories include **offensive**, **illicit** and **extremism**.* "

1.56.5. Our filter sends daily reports of any suspicious searches. These are viewed by the Network Manager and DSL. The DSL will investigate further, if required.

1.56.6. Our filter holds report information for 7 days, any investigations requiring filter report information must be requested within this time. All staff and pupil know how to report instances of inappropriate computer or internet use and aware that this must be done immediately. (Staff can report instances of computer or internet misuse to the Network Manager or ICT TA, either in person, completing a helpdesk support ticket or through email to a support email address. If this is not possible or the instance is severe the member of staff can go straight to the Head of School/DSL. Pupils can report instances of computer or internet misuse to any member of staff who can then follow the staff process.)

1.56.7. Changes to the filtering are made by the Network Manager. Any member of staff can request a website to be unfiltered and must provide a reason. This can be done in person, but is recommended that it is requested by email or support ticket with the website listed. The Network Manager will then review the site and check that it is appropriate for educational purposes. If deemed appropriate it will be unfiltered for the relevant filtering policies. A log of this will be kept by the Network Manager to be reviewed by the Online Safety Group.

1.56.8. **Assessing risks**

1.56.9. The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked Internet content, it is not possible to guarantee that unsuitable material will never appear on an Academy device. The Academy cannot accept liability for the material accessed, or any consequences of internet access.

1.56.10. The Academy will give responsibility to the Network Manager to monitor the use of Internet, email and messaging services.

1.56.11. The Academy should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate through the Online Safety Group.

1.57. **Handling Online Safety complaints**

1.57.1. Complaints of Internet misuse will be dealt with by the Network Manager and escalated as a safeguarding concern to the DSL, e.g. Cyberbullying.

1.57.2. Any complaint about staff misuse must be referred to the Head of School, unless it is the Head of School in which case it must be referred to the Principal;

1.57.3. Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures (see Child Protection & Safeguarding Policy).

1.57.4. Pupils and parents will be informed of the possible consequences for pupils misusing the Internet.

1.57.5. Pupils and parents will be informed of the complaints procedure.

1.57.6. Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

1.58. **Enlisting parents' support**

1.58.1. Parents' attention will be drawn to the Academy Online Safety Policy in newsletters and on the Academy website.

1.58.2. Parents will be given a copy of the Acceptable Use Agreement that their child has signed. They will be encouraged and supported to monitor their children's use of technology at home.

1.58.3. The Academy will provide regular Online Safety advice for parents through the school website, newsletters and free publications.

1.58.4. Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: https://www.childnet.com/ufiles/Information-for-Parents-and-Carers.pdf

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Visitors and members of the community

1.59. Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, the relevant AUA, and expected to read and follow them.

1.61**. Cyber-bullying**

1.61.1. **Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

1.61.2. **Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

For more information on the signs of cyberbullying please refer to our Anti-Bullying Policy.

1.62. **Examining electronic devices**

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

1.63. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Staff should not use any external storage device unless it has been provided by the Network manager.

All portable staff devices must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

Work devices must be used solely for work activities.

Work devices are for the express use of the member of staff and not for use by anyone else in their household.

1.64. **How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

1.65. **Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, newsletters and staff meetings).

The DSL and Deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Annex 1 – Online Safety Glossary

The definitions used in the Online Safety Policy are:

Acceptable Use Policy: A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications services, such as mobile technology, can be used on the school premises.

App: A self-contained program or piece of software designed to fulfil a particular purpose; an application, especially as downloaded by a user to a mobile device.

Avatar: A graphic identity selected by a user to represent him/herself to the other parties in a chat-room or when using instant messaging.

Chat-room: An area on the Internet or other computer network where users can communicate in real time, often about a specific topic.

Digital Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Filtering: A method used to prevent or block users' access to unsuitable material on the Internet.

Instant messaging (IM)/ Direct messaging (DM): A type of communications service that enables you to create a kind of private chat room with another individual/group in order to communicate in real time over the Internet, using text or voice based communication.

Malware: Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

Peer-to-peer (P2P): A peer-to-peer network allows other users to directly access files and folders on each other's computer. These networks such as 'Limewire' can create weaknesses in networks security by allowing outside users access to the schools resources.

Ransomware: Ransomware is a type of malware program that infects, locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner. Ransomware may also be referred to as a crypto-virus, crypto-Trojan or crypto-worm.

Spam: Unsolicited junk messages. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

SWGfL: South West Grid for Learning - A not-for-profit charitable trust, providing a wide range of products, services and solutions designed specifically for education, (e.g. Online Safety advice and training).

Video Conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video (e.g. Skype and Facetime).

Virus: A computer program that enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam: A webcam is a camera connected to a computer, or incorporated in a device, that is connected to the Internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.