



Online Safety Policy

Review frequency:	Annually
Last reviewed:	Sept 2023
Agreed by Trustees:	Sept 2023
Next review date:	Sept 2024

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside of school:

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- School devices are for the express use of the individual who has been assigned the device and not for use by anyone else in their household.
- Installing anti-virus and anti-spyware software (to be done by the Network Manager)
- Keeping operating systems up to date by always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.
- Staff and pupils should not use any external storage device unless it has been provided by the Network manager.

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

How the Academy will respond to issues of misuse:

Where a pupil misuses the Academy'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 Academy'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.

Filtering:

- 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.
- The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Our filters send reports of any suspicious searches. These are viewed by the Network Manager/ICT TA and DSL. The DSL will investigate further, if required.
- All staff and pupils know how to report instances of inappropriate computer or internet use and are 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, 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.)
- 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.
- In line with KCSIE 2023, parents, governors and staff receive information about our filtering systems for in school and for school devices outside of school. We use our termly online safety and computing newsletters to communicate this information and governing body meetings to discuss wider issues concerning online safety.
- Our filtering system relies on daily-updated filter lists from the IWF and Counter Terrorism Policing's CTIRU within the Metropolitan Police Service. This ensures strict adherence to PREVENT guidelines, with monthly updates directly from CTIRU.
- Our filtering provider is officially recognized as an appropriate filtering service by the UK Safer Internet Centre

These comprehensive measures collectively ensure our strict compliance with the revised KCSIE (September 2023) Annex C guidelines.

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, e-bulletins and staff meetings). As part of these sessions, online safety and safeguarding will be included.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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.

Monitoring Arrangements:

The DSL logs behaviour and safeguarding issues related to online safety on our Provision Map portal.

This policy will be reviewed every year by a member of the SLT. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links to other policies:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy and privacy notices

- Complaints procedure
- ICT and internet acceptable use policy
- Anti-Bullying
- Mobile Phone policy

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

- UK Safer Internet Centre:
<https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Childnet International:
<http://www.childnet.com/parents-and-carers/hot-topics>
- Internet Matters:
<https://www.internetmatters.org/>
- ThinkUKNow (CEOP)
<https://www.thinkuknow.co.uk/>

Roles and Responsibilities

Title	Body	Name
Safeguarding Governor	St Issey School	Marjorie Smith
Designated Safeguarding Lead	St Issey School	Chris Parham
Deputy Designated Safeguarding Lead	St Issey School	Sarah Sole
Safeguarding Governor	Trevithick Learning Academy	Joe Parma
Designated Safeguarding Lead	Trevithick Learning Academy	Will Johnson
Deputy Designated Safeguarding Leads	Trevithick Learning Academy	Kirsty Hitchens Melanie Wells Chris Sevier Nicola Garge



Key Stage One Acceptable Use Agreement

This is how we stay safe when we use school devices:

- I will ask a teacher or suitable adult if I want to use a device.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of school devices.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a school device.
- I will not share my username and password or any other private information with anyone.

To be completed by a parent/guardian & returned to school:

Child's name : _____

Parent/Guardian name: _____

Parent/Guardian signature: _____



Key Stage Two Acceptable Use Agreement

- I will only access computing equipment when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure; this includes not sharing it with others.
- I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
- I will always use my own username and password to access the school network and subscription services such as Purple Mash.
- In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- I will use all communication tools carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- Before I share, post or reply to anything online, I will T.H.I.N.K.

T = is it true?
H = is it helpful?
I = is it inspiring?
N = is it necessary?
K = is it kind?

- I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken

I understand this agreement and know the consequences if I don't follow it.

My Name:





Class:

Parent/Carer Signed:

Today's Date:



EYFS Acceptable Use Agreement

 <p>✓ I ask before I use a tablet, computer or camera.</p>	 <p>✓ I tap or click on things I have been shown.</p>
 <p>✓ I check if I can tap/click on things I haven't seen before.</p>	 <p>✓ I tell a grown-up if something upsets me.</p>
My Name: <input type="text"/>	Class: <input type="text"/>
Parent/Carer Signed: <input type="text"/>	Today's Date: <input type="text"/>