

THE FEDERATION OF TROSNANT SCHOOLS

Stockheath Lane, Havant, PO9 3BD Tel: 023 92475606 Fax: 023 92499423
Email: adminoffice@trosnant.hants.sch.uk Website: www.trosnantschools.co.uk

Executive Headteacher - Ian Waine
Executive Deputy Headteacher - Clive Mulligan



POLICY:

Drafted by:	IT Lead 2021
Reviewed by:	IT Lead 2025
Approved by Governing Body:	FGB – Sept 2025
Implementation:	Immediate
Review:	July 2026

Online Safety Policy

The online safety policy needs to be read in conjunction with the Safeguarding, AI, Acceptable Use of ICT, Curriculum, PSHE, RSE, Anti-Bullying, Data Protection, GDPR and Behaviour Policies.

This policy has been written in light of the following reviews and guidance:

- MoPP example policies (2015)
- Children's Online Activities, Risks and Safety: A Literature Review by the UKCCIS Evidence Group (Oct 2017)
- Growing Up Digital: A Report of the Growing Up of Digital Taskforce by the Children's Commissioner (Jan 2017)
- The Internet Safety Strategy Green Paper (Oct 2017).
- Vulnerable Children in a Digital world (2018)
- Teaching Online Safety in Schools (January 2023)

Keeping Everyone Safe: Education

Education of Pupils

Whilst regulation and technical solutions are very important, device use must be balanced by educating *pupils* to take a responsible approach. The education of pupils in online safety is therefore an essential part of Trosnant's online safety provision. Children and young people need help and support to recognise, avoid and react to online safety risks and build their resilience.

Online safety should be embedded in all areas of the curriculum and staff should provide continuous opportunities for online safety discussions. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and will be provided in the following ways:

- A planned online safety curriculum provided as part of the Computing Scheme of work (Purple Mash) to be taught every Autumn term and knowledge 'recalled' during all computing lessons throughout the academic year.
- Further learning is provided by the PSHE and new RSE curriculum (supported by SCARF).
- A planned programme of PDL assemblies and tutorial/pastoral activities, utilising the Online College resources.
- Identification of pupils who may be vulnerable to HROS (high risk online scenarios), with planned and targeted interventions for those pupils.



Everyone will achieve their best!



THE FEDERATION OF TROSNANT SCHOOLS

Stockheath Lane, Havant, PO9 3BD Tel: 023 92475606 Fax: 023 92499423
Email: adminoffice@trosnant.hants.sch.uk Website: www.trosnantschools.co.uk



Executive Headteacher - Ian Waine
Executive Deputy Headteacher - Clive Mulligan

Skills

Pupils will be taught to question, understand, analyse and respond to the following online safety topics. Over the course of their time with us, pupils will develop the ability to make reasoned, informed online choices and the resilience to cope with the challenges of life in a digital world.

Age restrictions	Cookies	Disinformation	Fake websites	Harvesting and farming
Verification	Copyright	Hoaxes and scams	Fraud and phishing	Keylogging
Digital footprints	Permissions	Authenticity	Credentials	Data collection
Hacking	Platforms	Notifications	Online challenges	Persuasive design
Clickbait	Flaming	Grooming	Live streaming	Social media & mental health
Reputation	Validity	Anonymity	Invisibility	Self-image and identity
Screen time	Advertising	In-app purchases	Communication	Gender stereotypes
Online abuse – intimidation, trolling, bullying, harassment, emotional, hate crime, blackmail				

Lessons and Teaching

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons, where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Staff should create an environment where pupils feel safe to discuss their own experiences online. Discussions should be promoted and valued (for concerns, see reporting guidance below).

Education of Parents

With the current speed of on-line change, some parents and carers have only a limited understanding of online risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often their children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Some of the risks could be:

- unwanted contact
- grooming
- online bullying including sexting
- digital footprint
- accessing and generating inappropriate content

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, leaflets, social media
- Parent-teacher meetings



Everyone will achieve their best!



THE FEDERATION OF TROSNANT SCHOOLS

Stockheath Lane, Havant, PO9 3BD Tel: 023 92475606 Fax: 023 92499423
Email: adminoffice@trosnant.hants.sch.uk Website: www.trosnantschools.co.uk



Executive Headteacher - Ian Waine
Executive Deputy Headteacher - Clive Mulligan

- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites and publications
- Presentations e.g. parent workshops
- Urgent information via e-mail/SMS direct to parents

Education of Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An audit of the online safety training needs of all staff will be carried out regularly, through performance management and staff drop-in sessions.
- All new staff should receive online safety training as part of their induction programme (through the National College), ensuring that they fully understand the school Online Safety Policy, AI Policy and Acceptable Use Agreements.
- The Online Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and/or INSET days.
- The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required, and to teaching staff during staff meetings/INSET days. The Online Safety Coordinator may also provide training for LSAs at their meetings.

Keeping Pupils Safe: School Systems and Permissions

Flexible Web Filtering

The school use Agile ICT for their internet provision and flexible web filtering (changed from HCC in July 2017). They in turn, use Fortigate (developed by Fortinet) to ensure school and pupils are kept safe.

"The Fortigate is set up to be compliant with the DfE's Safeguarding policy as standard for all users, with appropriate configurations for various groups of users such as Teachers, Admin, Pupils etc. This is updated on a regular basis centrally by Fortinet. Fortinet is a member of the IWF and the solution blocks access to illegal Child Abuse Images and Content (CAIC). The Fortigate solution Blocks and Monitors Illegal Content, Child Sexual Exploitation, Discrimination/Bullying, Drugs/Substance Abuse, Extremism, Pornography, Self-Harm/Violence. The FortiGate integrates with the police assessed list of unlawful terrorist content, produced on behalf of the Home Office and blocks access to any sites relating to Extremism and/or Terrorism."

Any websites can be added to the list of blocked websites when reported to Agile. The computing lead and business manager receive weekly monitoring reports regarding any access made by a user that is deemed to be of concern. These will be logged and any action taken as necessary, with relevant staff informed.

Pupils do have access to Google Images as these are vital tools when used for educational purposes. It is therefore paramount that staff remain vigilant at all times when children are accessing these sites under their care. **It is not permitted for children to use the internet or devices at break times and lunch times unless supervised.**



Everyone will achieve their best!



THE FEDERATION OF TROSNANT SCHOOLS

Stockheath Lane, Havant, PO9 3BD Tel: 023 92475606 Fax: 023 92499423
Email: adminoffice@trosnant.hants.sch.uk Website: www.trosnantschools.co.uk

Executive Headteacher - Ian Waine
Executive Deputy Headteacher - Clive Mulligan



Publishing of Images

Images of children, either with or without full names, are not to be published anywhere without the permission of parents or carers. Where the parents have signed a consent form to allow images to be used in the past, this must be confirmed as circumstances often change. They must also be informed of the reason or purpose for the use of the image.

Social media

Personal social media and networking sites are not permitted on site using school equipment and technology. Staff may still access websites such as Facebook on site using their own personal equipment which is NOT connected to the server. They must use this privilege in accordance with the guidance outline in the 'Acceptable Use of ICT' policy. Information, photos and posts about pupils or staff at the school are not permitted and the user will be asked to remove them. Failure to do so may result in disciplinary action.

School's Facebook and Instagram accounts are monitored and updated regularly by our admin staff. Staff are required to follow safeguarding procedures regarding the uploading of photos of pupils, only those with consent to be feature on Social media should appear.

Mobile phones

We understand the need for children (particularly those who walk to and from school alone) to bring mobile phones to school. Any mobile phones, iPods, tablets etc must be labelled and handed into the class teacher until 3:15pm. They are not to be used during school hours. In addition, children should not wear smart watches in school as these are expensive devices and may contain technology and communication software that is not appropriate for school. Staff phones may not be used to take pictures of children or their work.

Where children need to have their mobile device with them in school for a particular reason – e.g. to access a medical app – the class teacher and parent should make it clear to the child that they must not access their phone for any other reason. Parents should not use the mobile device to contact their child. The parent/carer will in addition be asked to sign a consent form. (Appendix 1) The parent/carer should check the mobile device and report any other activity to the school e.g. taking photographs, accessing the internet in school to ensure safeguarding.

Keeping Staff Safe

The guidance given here is IN ADDITION to the information and recommendations given for staff in the 'Acceptable Use of ICT' policy. Please accept this list of 'Do's' and 'Don'ts' that has been provided by Hampshire County Council, which outlines practical things you can do to keep yourself safe online.

- I will ensure that I understand how any site I use operates and therefore the risks associated with using the site.
- I will check what images and information is held about me online by undertaking periodic searches of social networking sites and using internet search engines.
- I understand that when publishing information about myself and images of myself online these will end up in the public domain.
- I will answer my mobile telephone with 'Hello' rather than my name, if the number on the display is unknown to me.



THE FEDERATION OF TROSNANT SCHOOLS

Stockheath Lane, Havant, PO9 3BD Tel: 023 92475606 Fax: 023 92499423
Email: adminoffice@trosnant.hants.sch.uk Website: www.trosnantschools.co.uk

Executive Headteacher - Ian Waine
Executive Deputy Headteacher - Clive Mulligan



- I will take screen prints and retain text messages, emails or voice mail messages as evidence of any harassment or improper behaviour towards me. I will report all incidents of cyberbullying arising out of my employment to my Head teacher. I will report any threatening or intimidating behaviour to the police for them to investigate.
- I know I should not allow any cyberbullying to continue by ignoring it and hoping it will go away.
- I know I should not return emails, telephone calls or messages or retaliate personally to the bullying.
- I know I should seek to have offensive online material removed through contact with the site, once screens have been captured as evidence.
- I will seek support from my manager, professional association/trade union, friend, or employee support line as necessary.
- I know I can access and use the DCSF guidance on Cyberbullying, specifically the advice on reporting abuse and removal of material/blocking the bully's number/email (see attachment/link below)
- I know I should not put information or images on-line, take information into school, or share them with colleagues, pupils or parents (either on site or off site) when the nature of the material may be controversial.
- I know that my school passwords and sensitive information needs to be kept safe.
- I will therefore not transport data or files between school and home using a memory stick, and I will not store information on any type of cloud services. Agile ICT provide school with a Remote Working Server allowing us to access the server from home. This is available to anyone who wishes to use it.
- I know I can find out what data and personal information is being held about me under 'The Data Protection Act 1998.'

Keeping Everyone Safe: Reporting Incidents

Children

Pupils need to feel confident to report issues and we must create an environment where they feel safe to do so. Class teachers may be able to address the child's issue within whole class activities, or we may need to speak to the child directly. Any concerns that staff have about a pupil in their care have a duty to report this. Depending on the severity of the incident, this must be reported to either the online safety coordinator, a DSL or a member of SLT. Concerns must be recorded on CPOMS, ensuring the "online safety" tag is selected.

Any grooming concerns will need to be reported to the parents (providing the parent is not the perpetrator) and the police immediately.

Staff

Staff also have a duty to each other to give reminders and advice about keeping safe online. It is good practice to share this knowledge and understanding.

It is a collective responsibility to ensure we are using technology safely, and that we are giving the children the correct tools to keep themselves safe at school and at home. Please speak to the online safety coordinator about any concerns re: websites, equipment or access. Website concerns may then be reported to CEOP.

I have read, understand and accept the Online Safety policy, and know what I need to do to keep myself and the children I work with safe. I have centrally signed for this document and acknowledge my receipt of it.

Written by Claire Louth, June 2021. Reviewed by Laura Jacobs, June 2024



Everyone will achieve their best!



THE FEDERATION OF TROSNANT SCHOOLS

Stockheath Lane, Havant, PO9 3BD Tel: 023 92475606 Fax: 023 92499423
Email: adminoffice@trosnant.hants.sch.uk Website: www.trosnantschools.co.uk

Executive Headteacher - Ian Waine
Executive Deputy Headteacher - Clive Mulligan



Online Safety Policy

Appendix 1: Parent Carer Consent Form

With Reference to:

Mobile phones

Where children need to have their mobile device with them in school for a particular reason – e.g. to access a medical app – the class teacher and parent should make it clear to the child that they must not access their phone for any other reason. Parents should not use the mobile device to contact their child. The parent/carer will in addition be asked to sign a consent form. (Appendix 1) The parent/carer should check the mobile device and report any other activity to the school e.g. taking photographs, accessing the internet in school to ensure safeguarding.

Child's name:

DOB:

Medical Condition:

Name of Medical App:

I confirm that my child requires a mobile phone with them at all times in school in order to access an app or GPS for medical reasons. I understand that I must not use my child's mobile device to contact them and that any contact should be through the school office. I will check the device regularly and report any other 'in-school use'.

I confirm I have explained to my child, and that I believe they understand, that they are trusted to not use the mobile device in school for any other purpose.

Parent Carer Signature:

Parent Carer Name:

Date:



Everyone will achieve their best!

