The Schools of Woolton Hill

ONLINE SAFETY POLICY

January 2023

Reviewed by Paul Davies

Approved by Governing Body: January 2023

Next Review: January 2024

Online Safety Policy

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 our 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.
- Further learning is provided by the PSHE and new RSE curriculum (supported by SCARF)
- A planned programme of assemblies and 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.

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 (e.g. 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

Many parents and carers have only a limited understanding of online safety 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 children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, leaflets, blogs, social media
- Parent-teacher meetings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites and publications
- Presentations by the Digital Leaders
- Urgent information vis 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 ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The DSLs 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 DSLs 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 Harrap ICT for their internet provision and flexible web filtering.

Any websites can be added to the list of blocked websites when reported to Harrap.

When pupils do have access to You Tube and Google Images (as these are vital tools when used for educational purposes) It is 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.

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

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.

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 to the Admin Team in the Office. 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.

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.
- 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. Harrap 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.