Online Safety Policy

Written by:	Samantha Britt (Computing Leader)
Review Cycle:	Every Three Years
Next Review:	Autumn 2026
Statutory / Non-Statutory:	Non-Statutory
Last Reviewed:	Autumn 2023

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance,

Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

Roles and Responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety records as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see Appendix)

The Headteacher/Designated Safeguarding Lead

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. As DSL, they also take a lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with other leaders and staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are recorded (on CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are recorded (on CPOMS) and dealt with appropriately in line with the behaviour for learning policy
- Updating and delivering staff training on online safety

Online safety incidents could include, but are not restricted to: using another person's username and password; using technology to upset or bully; attempting to access websites that you do not have permission to access.

Liaising with other agencies and/or external services if necessary, including Schools Broadband, Drift IT Services and Hampshire County Council to achieve the following:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. The school's Netsweeper Filtering software is provided by Schools Broadband.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly. All school computers/laptops/servers have ESET anti-virus installed.
- Conducting a full security check and monitoring the school's ICT systems. Drift IT Services check the ESET anti-virus, on a monthly basis, and a report is issued to the school's admin office.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files. ESET anti-virus actively scans all files, including downloaded files. Should they show as suspicious or dangerous, ESET quarantines the files and computers can be quarantined from the network to stop any wide-spread issues.

Staff, Volunteers, and Visitors

All staff, including contractors and agency staff, volunteers and visitors are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL (or deputies) to ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy
- If staff or pupils discover an unsuitable site, it must be reported via email to Mrs L Morris (adminoffice@woodcot.hants.sch.uk) who will report it to Drift IT Services
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Behaviour and Relationship Policy

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Support their child to understand and adhere to our terms of acceptable use of the school's ICT system and internet

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

- UK Safer Internet Centre - Helping children stay safe online
- Childnet International - Make the internet a great and safe place for children
- Disrespect Nobody - Healthy online relationships

Educating Parents About Online Safety

The school will raise parents' awareness of internet safety, including cyber bullying, via newsletters, our website and Facebook page. Our Family Support Co-ordinator can signpost parents to support as necessary. This policy will also be published on the website.

Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum:

We teach children about:

- Keeping safe online
- Self-image and identity
- Image sharing
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Evaluating the authenticity of information found online
- Privacy and Security

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers, governors and pupils are expected to follow the acceptable use of the school's ICT systems and the internet as outlined in Appendix 1 and 2.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We may monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Mobile Devices

Adults should not use their mobile devices around children and pupils who bring mobile devices into school must leave them in the school office and collect them at the end of the day.

Staff Using Work Devices Outside 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
- 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
- Not sharing the device among family or friends

- Staff members must not use the device in any way which would violate the school's terms of acceptable use.

If staff have any concerns over the security of their device, they must seek advice from Drift, our IT services provider.

How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, this will be managed in line with our Behaviour and Relationship Policy.

If 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 line with the school's Staff Code of Conduct.

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

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 and staff meetings).

The DSL will undertake Designated Safeguarding Lead (DSL) training, at least every two years and Child Protection and Safeguarding training, every year, both of which will include online safety. 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.

Cyber-bullying

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.

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.

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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour and Relationship 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.

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 and parents will be informed.

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

This policy was written in conjunction with Woodcot Primary School's Computing, PSHE and Safeguarding Curriculum.

Linked Policies:

- Anti-bullying Policy
- Behaviour and Relationship Policy
- Child Protection and Safeguarding Policy
- Acceptable Use of ICT Policy

Appendix 1 - What does acceptable use for pupils look like?

As a pupil at Woodcot Primary School, I will:

✓ Ask a teacher or adult if I can use a computer or device before using them

✓ Only use websites that a teacher or adult has told me or allowed me to use

✓ Tell my teacher immediately if:

- I click on a website by mistake
- I receive messages from people I don't know
- I find anything that may upset or harm me or my friends

✓ Use school computers for school work only

✓ Always use the school's ICT systems and the internet responsibly and for educational purposes only

✓ Only use them when a teacher is present, or with a teacher's permission

✓ Be kind to others and not upset or be rude to them

✓ Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly

✓ Only use the username and password I have been given, & keep my username and passwords safe and not share these with others

✓ Try my hardest to remember my username and password

✓ Never share my password with anyone, including my friends

✓ Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer

✓ Check with my teacher before I print anything

✓ Log off or shut down a computer when I have finished using it

✓ If I bring a personal mobile phone to school, I will not use it whilst at school or on school grounds and I will leave it in school office.

I will not:

✓ Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity

✓ Open any attachments in emails, or follow any links in emails, without first checking with a teacher

✓ Use any inappropriate language when communicating online, including in emails

✓ Log in to the school's network using someone else's details

✓ Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Appendix 2 - What does acceptable use for adults look like?

As an adult working at Woodcot Primary School, I will:

✓ Only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role

✓ Agree that the school may monitor the websites I visit and my use of the school's ICT facilities and systems

✓ Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy

✓ Let the designated safeguarding lead (DSL) and Computing Leader know if a pupil informs me they have found any material which might upset, distress or harm them or others,
and will also do so if I encounter any such material.

✓ Use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will not:

✓ Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)

✓ Use them in any way which could harm the school's reputation

✓ Access social networking sites or chat rooms

✓ Use any improper language when communicating online, including in emails or other messaging services

✓ Install any unauthorised software, or connect unauthorised hardware or devices to the school's network

✓ Share my password with others or log in to the school's network using someone else's details

✓ Take photographs of pupils without checking with teachers first

✓ Share confidential information about the school, its pupils or staff, or other members of the community

✓ Access, modify or share data I'm not authorised to access, modify or share

✓ Promote private businesses, unless that business is directly related to the school