Warden Hill
PRIMARY SCHOOL

Online Safety Policy

Member(s) of staff responsible	Computing Team
Governor responsible	Chair of Standards committee
Date agreed with staff	September 2023
Full Governors	25/10/23
Frequency of policy review	Annual
Date next review due	Sep 2024

Document Version Control

Issue Number	Issue Date	Summary of Changes
1.0	January 2008	Original issue
2.0	September 2011	Reviewed – updated in line with current best practice
2.1	September 2012	Reviewed – no changes
2.2	September 2013	Reviewed by PH, TC and GF – no changes
2.3	November 2014	Reviewed
2.4	December 2015	Reviewed – updated in line with current best practice
2.5	December 2017	Reviewed – updated in line with current best practice
2.6	January 2019	Content updated – now made a stand-alone policy and removed from AUP.
2.7	September 2020	Updated to include 3 types of risk
2.8	September 2022	Updated to include 4 types of risk Additions and amendments made to reflect KCSIE updates
2.9	September 2023	Additions and amendments made to reflect KCSIE updates

Contents

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for children to be more creative and productive in their work. Whilst our school fully supports and promotes the use of technology, it is imperative that it is used in an acceptable and safe manner at all times.

1) Aims

The aims of our Online Safety policy are 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.

2) Legislation and Guidance

This policy is based on the Department for Education's 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 headteacher's and school staff, relationships and sex education, searching, screening and confiscation. It also refers to the Department'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 takes into account the National Curriculum computing programmes of study.

3) Roles and Responsibilities

The Governing Body

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

All governors will:

- Ensure that they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (see Acceptable Useage Policy).
- Ensure that online safety is a running and interrelated theme.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Supporting the Headteacher in making sure all staff are aware of the procedures to follow with regards to responding to online safety concerns, including online child-on-child abuse issues.
- Checking that appropriate filtering and monitoring systems are in place, which are updated on a regular basis. These aim to keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. Filtering and monitoring decisions must consider those who are 'potentially at greater risk of harm' and how often they access the IT system along with the proportionality of costs versus safeguarding risks.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Accessing relevant training to gain a clear understanding of the unique risks associated with online safety. Recognise the additional risks that pupils with SEND face online and have the relevant knowledge to keep children safe online.

- Working with the Headteacher, computing team and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety. This includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. Online safety needs to be addressed as part of regular child protection training (at least annually) and updates provided as necessary.
- Ensure all staff, including Governors, are provided with appropriate and up-to-date online safety information and training at induction and as part of regular child protection training and updates.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the governing board.

The computing team

The computing team are responsible for:

- Ensuring that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Ensuring the continual teaching of online safety to all pupils as part of the computing curriculum.
- Liaise with RSE Team to ensure pupils are taught about online safety as part of the statutory RSE curriculum. This must recognise that a more personalized or contextualized approach for more vulnerable children e.g. victims of abuse and SEND may be needed.

All staff and volunteers

All staff, including supply teachers, are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms of acceptable use of the school's ICT systems and the internet (see Acceptable Useage Policy) and ensuring that pupils follow the school's Acceptable Useage Policy.
- Working with the DSL/computing team to ensure that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here.'

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns of 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. A summary of these are included in the school's Computing Golden Rules which are revisited each year and during computing lessons.

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4) Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the computing curriculum and the statutory RSE curriculum.

In **Key Stage 1**, pupils will be taught to:

- 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 or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and 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, where appropriate, invite speakers to talk to pupils about this.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5) Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

The school will let parents know:

- What systems the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who (if anyone) their child will be interacting with online.

Where possible, the school will organise external speakers to provide presentations to parents to help keep them up to date with online safety.

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.

6) Types of Risk

Online safety means keeping children safe from 4 types of risk, known as the 4 Cs. These are:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Abuse can take place completely online, or online and physically.

7) 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. (See also the school behaviour policy)

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. This issue will be addressed as part of online safety 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.

All staff and governors 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 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.

8) ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

More information is set out in the Acceptable Usage Policy – Adults.

9) Staff using work devices outside school (primarily laptops or iPads)

All staff must take all reasonable steps to ensure the security of their work device when using it outside school. This includes:

- Keeping the device password protected
- Any USB devices containing data relating to the school must be encrypted.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keep operating systems up to date by always allowing/agreeing to the latests automatic updates

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 the computing team or Headteacher.

10) 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.

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

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

12) 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 relevant updates as required (for example through e-mails and staff meetings).

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.

13) Monitoring arrangements

The DSL and/or computing team logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 1.

The policy will be reviewed annually by the Headteacher and/or computing team. At every review, the policy will be shared with the governing body.

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.

14) Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Internet acceptable usage policies (adults and pupils)

APPENDIX ONE

Online Safety incident report log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident