Warden Hill
PRIMARY SCHOOL

Online Safety Policy

Member(s) of staff responsible	Computing Team
Governor responsible	Chair of standards committee
Date agreed with staff	April
Date discussed with pupils	Spring Term assemblies
Date agreed at Sub-Committee	April 2019
Frequency of policy review	Annual
Date next review due	January 2020

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

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 preventing and tackling bullying and 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).

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.
- Working with the headteacher, computing team and other staff, as necessary, to address any online safety issues or incidents.
- 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.
- 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:

- 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.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- 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.

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.

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.

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 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.

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.

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

6) Types of Risk

Online safety means keeping children safe from 3 types of risk, known as the 3 Cs. These are:

Contact: being subjected to harmful online interaction with other users, for example adults pretending to be children

Content: being exposed to illegal, inappropriate or harmful material, for example pornography, fake news, racist or radical views and extremist views

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

Online safety often overlaps with other safeguarding issues. For example, children may show potential signs of being sexually abused online.

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.

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.

8) Staff using work devices outside school

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the computing team or Headteacher.

9) 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.

10) 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).

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.

11) 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.

12) 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

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