The Holt School
Online Safety Policy

April 2018

Version	DATE	DESCRIPTION
1	November 2011	Policy review
2	April 2018	Policy review

Reviewed	April 2018
Responsibility	Ms K Royle
Committee	Standards & Curriculum
Review Date	April 2020

1 Scope of the Online Safety Policy

This policy applies to all members of the Holt community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the Holt School. The Online Safety Policy defines the requirements for training and education of pupils and staff when using internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate students and staff about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school issues Acceptable Use Policies to staff and students. The aim of them is to ensure good and safe practice in the used of new technologies for school purposes and to protect both staff and students from inappropriate use of new technologies.

This Online Safety Policy:

- replaces the previous e-safety Policy which has been revised and renamed as the School's Online Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole;
- will operate in conjunction with other school policies including those for ICT, Behaviour 4 Learning, Safeguarding, Curriculum Planning, and Health & Safety; and
- has been written by the school, based on guidance from Wokingham Borough Council, and supported using resources from The School Bus Website, which itself is based on government guidance and is considered a model of good practice nationally.

This Online Safety Policy and its implementation will be reviewed bi –annually.

2 Statement of Intent

At The Holt School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet and other digital and information technologies open up opportunities for students and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. The school is committed to providing a safe learning environment for all students and staff, and has implemented important controls to prevent any harmful risks.

3 Roles and Responsibilities

It is the responsibility of all staff to be alert to the possible harm to students or staff due to inappropriate internet access or use, both inside and outside of the school, and to report incidents to the Designated Safeguarding Lead ("DSL") and Head of Year as a priority. Teachers are responsible for ensuring that online safety issues are embedded into the curriculum and safe internet access is promoted at all times and are aware of their responsibilities regarding the use of the schools ICT resources via the Acceptable Use Policy.

The DSL is ultimately responsible for ensuring the day to day online safety in the school, and managing any issues that may arise. Alongside the head of PHSE and head of computing, the DSL is responsible for reviewing on line safety policies and providing relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach students about online safety. The DSL is also accountable for ensuring all staff are aware and understand procedures to report on line safety concerns.

The governing body is responsible for the approval of the online safety policy and reviewing the effectiveness of the policy.

The ICT managed service provider is responsible for ensuring the schools infrastructure is secure and not open to misuse or attack. It is important that the managed service provider is fully aware of the Holt's Online Safety Policy and Acceptable Use Agreements. It must ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed and that technical filtering policies are regularly reviewed and updated. The ICT managed service provider must monitor the use of Holt ICT resources and report any misuse or attempted misuse to the Headteachers or DSL as appropriate.

All students are aware of their responsibilities regarding the use of school based ICT systems and equipment and their expected behaviour via the Acceptable Use Policy. Cyber bullying incidents are reported in accordance to the school's Behaviour for Learning Policy.

4 Communicating the policy

4.1 Informing students of the Online Safety Policy

- Online Safety rules are discussed with the students at the start of each year and there is a copy of the Acceptable Use Policy shared on FROG and in rooms with computers.
- Students are informed that network and internet use is monitored.

4.2 Staff and the Online Safety policy

- All staff are given the School Online Safety Policy and the Staff Acceptable Use Policy on the commencement of their contract, and their importance explained.
- Staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use are supervised within their leadership structure and have clear procedures for reporting issues.

5 Teaching and Learning

5.1 Students

- A planned online safety curriculum will be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students / pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5.2 Parents/ Carers

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 on-line 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, Learning Platform
- Parent events / campaigns e.g. Safer Internet Day

5.3 Staff

All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the schools Online Safety Policy and Acceptable Use Agreements.

6 What will the consequences be for misuse of the internet?

6.1 Students

- As a school we expect students to adopt the same moral standards on-line as off-line and inappropriate use of the internet is fully integrated in our Behaviour for Learning Policy.
- Teachers have the power to discipline students who engage in misbehaviour with regards to internet use. This is done in line with the School's Behaviour for Learning Policy.
- Complaints of more serious internet misuse are dealt with by a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Any student who does not adhere to the rules outlined in the Acceptable Use Agreement and is found to be wilfully misusing the internet, may have their internet access suspended and their parents or carers informed.

6.2 Staff

- Any complaint about staff misuse will be referred to the Co-Headteachers.

In the event that any illegal material is found on the school's network, or evidence that suggests that illegal material was accessed, the police will be contacted.

7 Managing Resources

7.1 Information system security

- School ICT systems capacity and security are overseen, and reviewed regularly by our IT Support Team.
- Virus protection is updated regularly.
- Management systems (LAN School) are available to allow teachers and members of staff to control workstations and monitor students' activity, for use when considered appropriate.
- The school will work with the DfE and the internet service provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the online safety coordinator or network manager. They will decide if it should be reported to the internet service provider
- Effective filtering systems are established to eradicate any potential risks to students through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems are used, that are relevant to students' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to the risks.
- The network manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

7.2 E-mail

- Students may only use their school e-mail accounts when communicating with staff and other students in school and any external contacts related to school.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

7.3 Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or students' personal information will not be published.
- A member of the senior leadership team will take overall editorial responsibility and ensure that content is accurate and appropriate.

7.4 Publishing students' images and work

- Photographs that include students are selected carefully, with regard to relevant permissions as appropriate, before photographs of students are published on the school website or school run social media accounts.
- Students' work can only be published publicly with the permission of the student and parents.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff using personal equipment for taking photographs should ensure all images are transferred to school

storage and deleted from the personal device. The school accepts the advantages of staff using personal devices from time to time, for example on trips.

75 Social networking and personal publishing

- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

7.6 Mobile devices and hand held computers

- Students are authorised to use mobile devices during lessons when directed by a teacher, or during lunchtime, while seated only.
- Mobile devices are not permitted to be used at any other time by students.
- Staff using hand-held devices which have been provided by the school are subject to the same monitoring and filtering.