| E-safety Policy | |
|---|---|
| Last reviewed – Autumn 2018 | Date of next Review – Autumn 2020 |
| HEADTEACHER | Author:<br><br>SAHT - Transition and Child Protection |

**Contents**

## 1. Introduction

e-Safety is about enabling the school community to benefit as much as possible from the opportunities provided by the Internet and the technologies we use in everyday life. It's not just about the risks, and how we avoid them. It's about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities.
e-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- National Education Network standards and specifications.

An e-safety policy allows the school to demonstrate that not only do we acknowledge e-safety as an important issue for the school community, but also that we have made a considered attempt to embed e-safety into our approach to learning using technology.
An e-safety policy demonstrates how we have worked to achieve a balance between using technology to enhance learning and teaching, and putting appropriate safeguards in place.
The school's e-safety policy will operate in conjunction with other policies referred to at the end of this document.

## 2. Why is Internet use important?

The purpose of Internet use in school is to help raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.
Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction.
Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access
Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

## 3. Responsibilities of the School Community

We believe that e-safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

## 4. Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's e-safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by students.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages students to adopt safe and responsible behaviours in their use of technology in and out of school.

- Support the work of the e-safety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-safety activities.

## 5. Responsibilities of the Senior Leadership Team

- Develop and promote an e-safety culture within the school community.
- Support the e-safety coordinator in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to e-safety effectively.
- Receive and regularly review e-safety incident logs and be aware of the procedure to be followed should an e-safety incident occur in school.
- Take ultimate responsibility for the e-safety of the school community.

## 6. Responsibilities of the e-safety Coordinator

- Promote an awareness and commitment to e-safety throughout the school.
- Be the first point of contact in school on all e-safety matters.
- Create and maintain e-safety policies and procedures.
- Develop an understanding of current e-safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in e-safety issues
- Ensure that e-safety education is embedded across the curriculum.
- Ensure that e-safety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on e-safety issues to the Senior Leadership Team as appropriate
- Ensure an e-safety incident log is kept up-to-date.
- Liaise with the Designated Child Protection Officer to report all incidents where a child is at risk of harm

## 7. Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's e-safety policies and guidance.
- Read, understand and adhere to the school staff Acceptable Usage Policy.
- Develop and maintain an awareness of current e-safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed e-safety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Be aware of what to do if an e-safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

## 8. Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's e-safety policies and guidance.

- Read, understand and adhere to the school staff Acceptable Usage Policy.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school ICT system.
- Report any e-safety-related issues that come to their attention to the e-safety coordinator.
- Develop and maintain an awareness of current e-safety issues, legislation and guidance relevant to their work.
- Maintain a professional level of conduct in their personal use of technology at all times.

## 9. Responsibilities of Students

- Read, understand and adhere to the school pupil Acceptable Usage Policy.
- Help and support the school in creating e-safety practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for their own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by students outside school.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Understand what action to take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if they know someone to whom this is happening.
- Discuss e-safety issues with family and friends in an open and honest way.

## 10. Responsibilities of Parents and Carers

- Help and support the school in promoting e-safety.
- Read, understand and promote the school pupil Acceptable Usage Policy with their children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss e-safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the school if they have any concerns about their child's use of technology.

## 11. Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings.

- We will provide a series of specific e-safety-related lessons in every year group as part of the curriculum.
- We will celebrate and promote e-safety through a planned programme of assemblies and whole-school activities.
- We will discuss, remind or raise relevant e-safety messages with students routinely wherever suitable opportunities arise during lessons. These include the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will ensure that the use of Internet derived materials complies with copyright law
- Students will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- We will remind students about their responsibilities through an end-user Acceptable Usage Policy which will have to be accepted each time a student logs on.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

## 12. How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- include e-safety as part of the events on Progress Days
- include useful links and advice on e-safety on our school website
- provide parents with useful information from the ThinkUKnow and ChildNet websites
- include a section on e-safety in the home-school agreement

## 13. Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is safe and secure.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All users will agree with an end-user Acceptable Use Policy appropriate to their age and access before joining the school as part of the home-school agreement and each time they log on to the school network.
- Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- Students will access the Internet using an individual log-on, which they will keep secure from others. They will ensure they log-out after each session, and not allow students to access the Internet through their log-on. Whether supervised by a member of staff, or working independently, students will abide by the school Acceptable Usage Policy at all times.
- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow students to access the Internet through their log-on. They will abide by the school Acceptable Usage Policy at all times.
- Any administrator or master passwords for school ICT systems will be kept secure and available only to the ICT technicians.

## 14. Wireless Access

- The school is responsible for ensuring that access is safe and secure as reasonably possible.
- Connection to the wireless network is protected by at least the Wi-Fi Protected Access (WPA) authentication method requiring the input of a secure passphrase.
- The passphrase will be kept secure and available only to the ICT technicians.

## 15. Inappropriate content

- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the e-safety policy is adequate and if the implementation of the e-safety policy is appropriate. We will regularly review our Internet access provision, and consider new methods to identify, assess and minimize risks.
- To increase the safety of all staff and students at Worthing High school we use:

  **Securus**

  Securus helps protect staff and students form computer misuse. If any inappropriate words or images are shown on the screen, Securus will capture the screen and save the image in a central database. The database

is reviewed once a week by the Technical staff to ensure no bullying or inappropriate use of the school system.

**Safe Search**

"*SafeSearch is designed to screen sites that contain sexually explicit content and remove them from your search results. While no filter is 100% accurate, SafeSearch helps you to avoid content that you may prefer not to see or would rather your children did not stumble across.* "

The SafeSearch option is the default setting for every user and cannot be changed.

## 16. Filtering Internet access

- The school uses a filtered Internet through a range of services and software.
    - **HTTPS Inspection**
      HTTPS Inspection, allows our firewall to monitor secure HTTP traffic (HTTPS). This will prevent students accessing/bypassing the filtering system by going to inappropriate encrypted sites.
    - **Web Filtering – by Lightspeed**
      The school has an in house web filtering system called Lightspeed. It allows us to provide a varied degree of filtering according to the needs of the classes being taught.
    - **Web – Filtering – by manually typed URLs**
      If a web site is deemed inappropriate for school use (e.g. Facebook), then we can block the website by typing the URL into our web filtering server.
    - **Web Filtering – by URL Categories**
      Our Web filtering server allows us to block certain categories.

- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-safety coordinator.
- If users discover a website with potentially illegal content, this must be reported immediately to the e-safety coordinator. The school will report this to appropriate agencies including the filtering provider, Local Authority, Child Exploitation & Online Protection Centre (CEOP) or Internet Watch Foundation (IWF).
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

**Links to other policies**

Mobile Device Policy
Acceptable Use Policy
Data Protection Policy
Child Protection Policy
Network Policy