Heathside School
E Safety Policy

Staff Member with Responsibility:	A Shakespeare, Vice Principal
Reviewed by:	**Student Learning & Progress**
Reviewed Date:	Spring 2017
Next Review Due:	Spring 2020

1: Introduction

ICT plays a critical role in everyday life in the 21st century and is a powerful tool for enhancing teaching and learning.

The E Safety Policy aims to provide information and guidance to students, staff, parents, carers and governors on using internet technology safely and responsibly.

The policy also links to the Behaviour for Learning, Data Protection, Child Protection, Anti-bullying, ICT, Bring Your Own Device (BYOD) and Acceptable Use policies (staff and students). The BYOD policy can be found in Appendix 1.

2: Aims

- To provide guidance, information for all stakeholders.
- To have the appropriate mechanisms to intervene and support any incident where appropriate.
- To ensure that all staff can recognise and are aware of E Safety issues.
- To promote E Safety through teaching students how to gain the knowledge and understanding to keep themselves safe and how to take responsibility for their own and others' safety.
- To manage the transition from locked down systems to more managed systems in order to help students understand how to manage risk and bridge the gap between systems at school and the more open systems outside school.
- To systematically review and develop E Safety procedures, including training, to ensure that they have a positive impact on students' knowledge and understanding.

3: The role of parents and carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use digital technology in an appropriate way. We will support parents by providing regular information and guidance on Internet safety. Parents/Carers are responsible for:

- Reading and endorsing the Student Acceptable Use Policy in student planners.
- Understanding the importance of talking to their child about their online profiles regularly and taking all reasonable precautions to ensure that their children are using the ICT resources available to them at home safely.
- Reporting to the school any online incidents that have occurred during school time so that they can be dealt with quickly.
- Dealing with incidents that arise out of school time and liaising with the school as appropriate.

4: Teaching and Learning

- The use of digital technology is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Digital technology is a part of the statutory curriculum and a necessary tool for staff and students.
- Students will be taught what Internet use is acceptable and what is not and given clear guidance on safe use of the technology.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be shown how to publish and present information appropriately to a wider audience.
- Students will be educated about E Safety issues through PSHE, use of Guest speakers and assemblies. The Safeguarding notice board also provides additional information for students.
- The school will seek to ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught how to report offensive Internet content.

5: Managing Internet Data Access

Information system security

- The school ICT systems and security will be reviewed regularly.
- Virus/adware protection will be updated regularly.
- Students will be required to comply with the Acceptable Use Policy which is in student planners and appears on all student PCs when students log on.
- The school will ensure it has suitable network/client firewalls and rule sets to protect the internet network.
- Guest networks will be segregated from internal networks.
- Remote access will only be presented through specific and secure software solutions.

6: Online Communication

- Students and staff may only use their school email addresses for school/business.
- If they receive an offensive email, students and staff must report it to either the network manager or, for more serious incidents, to the E Safety Coordinator (Ms Shakespeare).
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Staff to student email communication must only take place via a school email address or from within the learning platform and should be compatible with their professional role.

- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The school will monitor how email from students to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

7: Published content and the school web site

- The contact details on the website should be the school address, email and telephone number. Staff emails are made available but no personal information will be published.
- The Network Manager and School Business Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images

- Students' full names will be avoided on the website or VLE, as appropriate, including in blogs, forums or wikis, particularly in association with photographs or other digital media.
- Written permission from parents or carers will be obtained before photographs or other digital media are published on the school website online or in the school newsletter.
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing on the VLE

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must not place personal photos on any network space.
- Students will be advised to use nicknames and avatars when using public social networking sites.
- Videos online will be posted via the Heathside YouTube channel and will be checked prior to posting.

8: Managing filtering

The school will work to ensure systems to protect pupils are reviewed and improved. It will ensure that all Internet access has age appropriate filtering which is checked regularly.

- If staff or students come across unsuitable online materials, the site must be reported to the network manager and E Safety Coordinator.
- Regular checks will be made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school uses software to detect inappropriate language, indecent images or possible child protection issues.
- Use of video services will be appropriately supervised for the students' age. It should be teacher led and used for teaching and learning purposes.

9: BYOD and mobile phones

- Bring Your Own Device (BYOD) is available for sixth formers. The E Safety policy will be made available to parents via the website and sixth form students are required to read and sign the BYOD policy before bringing in their own device. BYOD will be closely monitored and reviewed.
- The school has a strict policy on the use of mobile phones. Mobile phones and other devices will not be used during lessons or formal school time except as part of an educational activity and with the permission of the teacher. The sending of abusive or inappropriate text messages is forbidden. Students must also not take, use, share or distribute images of others without their permission.
- Staff will use a school phone where contact with parents and students is required e.g. on educational visits.

10: Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Student and staff data will be retained after students and staff leave in accordance with data protection guidelines.
- All staff must read and sign the Acceptable Use Policy as part of their induction to the school.
- Visitors not employed the school should read and sign a Guest Acceptable Use policy before being given access to the internet via school equipment.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.
- The Acceptable Use Policy (students) is in the student planner. Students are also required to click to agree to abide by the policy every time they log on.

11: Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. The school's filtering and software solutions are used to detect inappropriate misuse. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey County Council can accept liability for the material accessed, or any consequences of Internet access.

12: Handling E Safety complaints

- Complaints of Internet misuse will be dealt with by the Network Manager in the first instance. Serious cases of misuse will be dealt with in accordance with the school's behaviour policy and may be referred to the E Safety Coordinator or, in her absence, to the Principal.
- Any complaint about staff misuse will be referred initially to the E Safety Coordinator and will be dealt with by the Principal in line with the school's Disciplinary and Capability Policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of consequences for students misusing the Internet.

13: Communication and training

- Appropriate elements of the E Safety Policy will be shared with students.
- Students will be informed regularly that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e safety issues and how best to deal with them will be provided.
- Staff will be given regular updates and training on E Safety issues.
- New staff will be informed of the arrangements as part of their induction process.
- Parents and carers will be provided with useful information, links and guidance via the website and regular parental forums will be offered on Internet Safety.

Appendix 1

Heathside School
Bring Your Own Device (BYOD) Policy (Sixth Form only)

As new technologies continue to become available, they also provide many new and positive educational benefits for teaching and learning. To encourage the growth we are allowing students to bring their own technology into school and use them in lessons. This policy is in conjunction with the 'Student Acceptable Usage Policy' and 'Mobile Phone Usage Policy'.

Definition
For the purpose of BYOD, devices means any privately owned portable equipment such as laptops, smart phones, e-readers, tablets and any devices that are able to connect to the internet.

Security and damages
Heathside cannot take any responsibility in the unlikely event of damage or theft of personal devices brought into school. If a device is stolen or damaged, it will be handled through the school's policies similar to other personal belongings.

The Provision
Connections will only provide internet access to users who use this facility. Students who wish to save their work onto the school's internal will do this via e-mail, USB or a remote solution provided by the school.
The current coverage is targeted for building use only and is not accessible in the fields or playgrounds.
The school cannot provide support to personal devices however, may provide 'best efforts' to assist in gaining access to the wireless.

Usage
Students are only allowed to use their devices in classes with the teacher's permission and only for that specific lesson. Sixth Form students are able to use their devices in the common room and LRC.
Devices must always be on silent mode and never used in tests or exams.

Student Agreement
- The system should only be used for education research or study. Any misuse of the system and this provision can be taken away.
- Users must use their own network logon account to access the facility. These details should also not be handed out
- Students are required to ensure they back up their data and keeping their devices free of viruses. Work will be backed up if it is transferred to the network
- Internet usage is monitored
- Students who use this system must have also already agreed to the 'Student Acceptable Usage Policy' and Behaviour Policy to which this policy also applies. This can be found on the Heathside website (www.heathside.surrey.sch.uk).
- It is the school's responsibility to protect the school, the students and the internal systems from common dangers of a public network
- Internet access will be partly filtered however, facilities such as social networking may be available. We may limit connection speeds and intend for classroom use only
- Any changes or requests for the wireless network must be given to the Network Manager
- Charging will likely not be available so students must also ensure their devices are charged prior to coming into the school

Heathside School

Bring Your Own Device (BYOD) Agreement

The BYOD facility is a privilege and can be removed if I do not adhere to the 'Student Acceptable Usage Policy' or the 'BYOD Policy'. By signing this agreement I understand that my device if lost or stolen it is not the responsibility of the school

I understand that misuse will be referred initially to the E Safety Coordinator and will be dealt with in line with the school's Behaviour for Learning Policy. Activity which might be deemed to be criminal may be referred to the Local Authority Designated Officer (LADO) or the police.

Full Name: …… (Printed)

Signature: …… Date: ……