Hartford Church of England High School

E-Safety Policy

Date	Review date	Coordinator	Nominated Governor
October 2019	Autumn Term 2020	L Naylor	S Mills

We believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and take care of their own safety and security.

E-safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their online experience.

Aim

- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet both in school and at home.

Responsibility of the Policy and Procedure

Role of the Governing Body

The Governing Body has:

- Ensured that a member of SLT is responsible for e-safety
- Delegated powers and responsibilities to the Headteacher to ensure all school personnel and stakeholders are aware of and comply with this policy;
- Responsibility for ensuring funding is in place to support this policy;
- Responsibility for ensuring this policy and all policies are maintained and updated regularly;
- Responsibility for ensuring policies are made available to parents;
- Undertaken training in order to understand e-safety issues and procedures;
- Nominated a link governor to visit the school regularly, to liaise with the Headteacher and the coordinator and to report back to the Governing Body;
- Responsibility for the effective implementation, monitoring and evaluation of this policy

Role of the Headteacher

The Headteacher will:

- Ensure all school personnel, pupils and parents are aware of and comply with this policy;
- Work closely with the Governing Body and the coordinator to create a safe ICT learning environment by having in place:
  - an effective range of technological tools
  - clear roles and responsibilities
  - safe procedures
  - a comprehensive policy for pupils, staff and parents;
- ensure regular checks are made to ensure that the web filtering methods selected are appropriate, effective and responsible;
- work closely with the link governor and coordinator;
- provide guidance, support and training to all staff;
- monitor the effectiveness of this policy;

Role of the E-Safety Coordinator

The coordinator will:

- Undertake an e-safety audit in order to establish compliance with Local Authority guidance;
- Ensure that all Internet users are kept up to date with new guidance and procedures;
- Ensure regular checks are made to ensure that the web filtering methods selected are appropriate, effective and reasonable;
- Undertake risk assessments in order to reduce Internet misuse;
- Lead the development of this policy throughout the school;
- Work closely with the Headteacher and the nominated governor;
- Provide guidance and support to all staff;
- Provide training for all staff on induction and when the need arises;
- Keep up to date with new developments and resources;
- Review and monitor;
- Annually report to the Governing Body on the success and development of this policy

Role of Nominated Governor

The Nominated Governor will:

- Work closely with the Headteacher and the Coordinator;
- Undertake appropriate training;
- Ensure this policy and other linked policies are up to date;
- Ensure everyone connected with the school is aware of the policy;
- Report to the Governing Body every term;

Role of School Personnel

School personnel will;

- Comply with all aspects of this policy
- Undertake appropriate training;
- Before using any Internet resource in school must accept the terms of the 'Responsible Internet Use' statement;
- Be responsible for promoting and supporting safe behaviours with pupils;
- Promote e-safety procedures such as showing pupils how to deal with inappropriate material;
- Report any unsuitable website or material to the e-safety Coordinator;
- Will ensure that the use of Internet derived materials complies with copyright law;

Role of Pupils

Pupils will be aware of this policy and will be taught to:

- Be critically aware of the materials they read;
- Validate information before accepting its accuracy;
- Acknowledge the source of information used;
- Use the Internet for research;
- The meaning of safe internet access;
- Respect copyright when using Internet material in their own work;
- Report any offensive e-mail;
- Report any unsuitable website or material to the e-safety Coordinator;
- Treat others, their work and equipment with respect;
- Support the School Code of Conduct and guidance necessary to ensure the smooth running of the school;

Role of Parents/Carers

Parents/carers will:

- Be aware of and comply with this policy;
- Be asked to support the e-safety policy as part of the home school agreement
- Make their children aware of the e-safety policy

Internet Use

The school Internet access will:

- Be designed for pupil's use;
- Include school web filtering technology which is designed to protect pupils from unsafe materials on the internet;
- Provide web filtering which is reviewed annually and improved if necessary;
- Include web filtering appropriate to the age of pupils;
- Have virus protection software installed which will be updated regularly;

Authorising Internet Access

- Before using any school ICT resource, all pupils and staff must read and sign the 'Acceptable ICT Use Agreement' (see appendices 1 & 2).
- Parents must sign a consent form before their child has access to the Internet, as part of the home school agreement.
- An up to date record will be kept of all pupils and school personnel who have Internet access.

E-mail

Pupils must:

- Only use approved e-mail accounts;
- Report receiving any offensive e-mails;
- Not divulge theirs or others personal details;
- Not arrange to meet anyone via the e-mail;
- Seek authorisation to send a formal e-mail to an external organisation;
- Not take part in sending chain letters

Staff must:

- Only use approved email accounts for school purposes
- Immediately tell a member of SLT if they receive offensive email

School Website

Contact details on the website will be:

- The school address
- E-mail address
- Telephone number

The school website will not publish:

- Staff or pupil contact details
- The pictures of children without written consent of the parent/carer;
- The names of any pupils who are shown;
- Children's work without the permission of the pupil or the parent/carer

Social Networking and Personal Publishing & Social Media

Pupils will not be allowed access:

- To social networking sites except those that are part of an educational network or approved Learning Platform. The school does provide information via social media sites, but pupils are not allowed access during the school day
- To newsgroups unless an identified need has been approved

Social Networking

- Pupils will be advised never to give personal details of any kind which may identify them and/or their location
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Mobile Phones

- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Protocol.

Inappropriate Material

- Any inappropriate websites or material found by pupils or school personnel will be reported to the e-safety Coordinator who in turn will report to the Internet Service Provider.

Internet System Security

- New programs will be installed onto the network or stand-alone machines by school technicians only.
- Data record devices may not be used in school.
- Everyone must be aware that under the Computer Misuse Act 1990 the use of computer systems without permission or for inappropriate use could constitute a criminal offence.

Complaints

- The E-safety co-ordinator will deal with all complaints of Internet misuse by school personnel or pupils.
- Parents will be informed if their child has misused the Internet.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- The School Handbook/Prospectus
- The school website
- The Staff Handbook
- Meetings with parents such as introductory, transition, parent-teacher consultations;
- Communications with home such as newsletters, text messaging system;
- Reports such annual report to parents and Headteacher reports to the Governing Body
- Information displays in the school.

Training
All staff will have e-safety training triennially or when new staff are appointed and information updates as new information arises.

Monitoring the Effectiveness of the Policy
Annually (or when the need arises) the effectiveness of this policy will be reviewed by the coordinator, the Headteacher and the nominated governor and the necessary recommendations for improvement will be made to the Governors.

Appendix 1

Hartford Church of England High School
Student Acceptable Use Protocol Agreement

This Acceptable Use Protocol is intended to ensure:

- that students will be responsible users and stay safe while using the internet and other communications technologies (handheld devices e.g. mobile phones/ipods) for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Protocol Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- ✓ I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- ✓ I will look after my password – I will not share it, nor will I try to use any other person's username and password.
- ✓ I will be aware of "stranger danger", when I am communicating on-line.
- ✓ I will not disclose or share personal information about myself or others when on-line.
- ✓ I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- ✓ I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so
- ✓ I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- ✓ I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- ✓ I will not use ICT or handheld devices to take or distribute images of anyone without their permission.
- ✓ I understand that handheld devices should not be used in any manner or place that is disruptive to the normal routine of the school and must not disrupt classroom lessons, movement times, break or lunchtimes, other educational visits or activities, such as fixtures with ringtones, music or beeping.
- ✓ I will only use my personal hand held / external devices (mobile phones /ipods etc.) in school if I have permission from my head of house or pastoral manager. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- ✓ I understand that the school accepts no responsibility for replacing hand held/external devices which have been lost, stolen or damaged, either within school or whilst travelling to and from school, and suggests marking handheld/external devices clearly with their names.
- ✓ I will ensure that the Bluetooth function and other functions used to send and receive instant messages of a handheld device must be switched off at all times and not used to send images, files or group messages to other handheld devices.
- ✓ I will not open any attachments to emails, unless I know and trust the person /organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- ✓ I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- ✓ I will not use chat and social networking sites when in school, and out of school I will never give personal details or locations to unknown contacts.

When using the internet for research or recreation, I recognise that:

- ✓ I should ensure that I have permission to use the original work of others in my own work
- ✓ Where work is protected by copyright, I will not try to download copies (including music and videos)

- ✓ When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- ✓ I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- ✓ I understand that if I fail to comply with this Acceptable Use Protocol Agreement, I will be subject to disciplinary action. This may include the loss of access to the school network / internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police. This may include the handheld device/external device being confiscated by the teacher and taken to a secure place within the school office, and if the device has camera or image transfer facility parent/carer will be contacted and will have to collect the device from the office. After the third infringement of confiscation of the device. The school will withdraw the agreement to allow me to bring a handheld/external device into school for a period of time.
- ✓ I understand that if I refuse to hand over a handheld/external device I am infringing the above Protocol. Refusal may result in exclusion and withdrawal of the agreement to allow me to bring a handheld/external device into school.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school I CT systems.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Protocol (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student			
Group / Class			
Signed		Student Date	
Signed Parent/		Carer Date	

Appendix 2

HARTFORD CHURCH OF ENGLAND HIGH SCHOOL

Staff ICT Acceptable Use Protocol

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Protocol.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulations (GDPR) 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the e-safety policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator and/or the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Team as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. To ensure my professional position is not compromised when using social networking sites, I will not accept friend request from a person I believe to be a parent or student at my school. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- I will ensure that mobile phone and devices will be switched off or switched to 'silent' mode with pin code access, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances. Emergency calls will be taken through reception.

- I will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator or the Head Teacher.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure Protocol compliance.

The School may exercise its right to monitor the use of ~~i~~nformation systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Protocol and the School's Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the

School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Protocol.

Signed: ……..... Print Name: …… Date: ……..…

Accepted by: …….. Print Name: ……..…….