Herne Junior School Online Safety Policy

Updated January 2024

Introduction

The rapid development of technology is having an increased impact to our everyday lives. At Herne, we enjoy extending our pupil's learning experience using technology at every opportunity. However clear guidelines need to be established and adhered to, ensuring pupils, staff and parents are aware of the potential dangers of using technology, in particular electronic communication. Safe and courteous use of the internet, texting, email, and social media sites are areas that require specific education. This is known as Online Safety.

Online Safety highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. At Herne, we understand the responsibility to educate our pupils on online safety issues, teaching them the appropriate behaviour, attitude and skills to enable them to remain both safe and legal when using the internet and related technologies. With this in mind, our Computing curriculum has focused online safety lessons and core online safety themes are embedded throughout the academic year.

This online safety policy has four key sections: Roles and Responsibilities; Technology Use, Teaching and Learning and Information and Links. The school's online safety policy shall operate in conjunction with other policies including the Safeguarding and Computing and ICT Policies.

All staff and shareholders must abide by acceptable use agreements.

Roles and Responsibilities

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they shall:

- Review this policy at least annually and in response to any online safety incident to ensure that: the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher (who is also a member of the Local Safeguarding Children's Board) has overall responsibility for online safety within the school. The day-to-day management of this shall be delegated to the Online Safety Co-coordinator(s). The Headteacher shall ensure that:

- Online Safety training throughout the school is planned, up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, governing body and parents.
- The designated Online Safety Coordinators have had appropriate training in order to undertake their day-to-day duties.
- All Online - Safety incidents are dealt with promptly and appropriately.

Online Safety Coordinator(s)

Reporting to the Headteacher, the Online-Safety Coordinator(s) are responsible for the day-to-day delivery of online safety learning activities throughout the school. The Online Safety Coordinator shall:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and Governing body on all online-safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the Local Authority, IT technical support and other agencies as required.
- Provide support with any online-safety issues raised via CPOMS.
- Support the Senior Leadership Team in the completion of the Online-Safety Audit (Annex A)

IT Technical Support Staff

Reporting to the Headteacher the IT Technical Support Staff are responsible for delivery of effective, secure and safe IT Solutions for the school. The Technical support staff are responsible for:

- Ensuring any technical Online-Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose and operating correctly through liaison with the Local Authority.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online-Safety coordinator(s) and Headteacher.
- Ensuring Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Ensuring Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Ensuring Passwords are applied correctly to all staff. Passwords for staff shall be a minimum of 8 characters.
- Monitoring and reporting of documents stored on internal systems, internet and email use for both staff and pupils and report any inappropriate action to the Headteacher.
- Ensuring the IT System Administrator password is to be changed regularly.
- Supporting the school's Data Controller in accordance with the General Data Protection Regulation (GDPR).

All Staff

Staff shall ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher.
- Any online safety incident is captured within CPOMS and reported to the Headteacher or in his/her absence, to the Online-Safety Coordinators. If you are unsure, the matter is to be raised with the Online-Safety coordinators or the Headteacher to make a decision.
- Use of technology in lessons, in particular the use of the internet, has been checked to ensure age appropriate content.
- Where appropriate, staff should ensure they feel adequately informed to be able to deliver online-safety lessons to students.
- Passwords are regularly changed and machines locked when not in use.

- All data that is received or produced pertaining to the school and its staff and/or pupils, is properly stored, accessed and removed in accordance with our Data Protection Policy.
- When entering pupil names on internal communication (such as the diary or staff update) only initials and their class are to be used.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services shall be dealt with in accordance with the behaviour policy. Students are also made aware of the Computer Charter (Annex B), highlighting their rights and responsibilities.

Online-Safety is embedded into our curriculum; students shall be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware of how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will support parents to help them gain the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and workshops, the school will keep parents up to date with new and emerging Online-Safety risks, and will involve parents in strategies to ensure that students are empowered to make informed decisions.

It shall be made clear to Parents that the school needs rules in place to ensure that their child can be properly safeguarded. As such parents shall sign the student Acceptable ICT Use Policy before any access can be granted to school ICT equipment or services.

Technology Use

Managing Risk

Herne uses a range of devices including PC's, laptops, e-readers and tablets (android & iPads). In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – The school's Internet access is provided by Hampshire County Council (HCC) and includes filtering appropriate to the age of pupils. An additional filtering set is available on staff devices to allow access to additional resources. Sites such as Facebook, YouTube and Instagram are filtered accordingly. Note: There is still a small risk that inappropriate material may occasionally get through filters. This is managed through further guidelines for teachers and pupils are taught what to do if this happens. IT Support, working closely with HCC, is responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.
If staff or pupils discover an unsuitable site, it must be reported to the Hants IT ICT Services Help Desk by email itservicedesk@hants.gov.uk

Email Filtering – Herne use Outlook 365 as our email provider, which has embedded spam filtering and malware detection.

Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Local Authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Personal data shall be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the new GDPR framework.

Passwords – All staff shall be unable to access most devices without a unique username and password. Staff will change their password if there has been a compromise. IT Support is responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices shall have anti-virus software. This software shall be updated at least weekly for new virus definitions. IT Support is responsible for ensuring this task is carried out, and shall report to the Headteacher if there are any concerns.

Safe Use

Internet – Internet use is part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use shall be granted to: staff upon signing the staff Acceptable Use Policy and pupils upon signing and returning their acceptance of the Acceptable Use Policy. Students must request permission before using the internet and only access sites approved by staff. Note: Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted unless permission has been granted by the Senior Management Team. Staff are not permitted to email students using personal email accounts.

Pupils are permitted to use the school email system for internal emails only, and as such can be given their own email address when it is required as part of the curriculum. Any breach of use shall result in suspension of their email account for an agreed time frame. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. The forwarding of chain letters is not permitted.

E-mails sent to an external organization should be written carefully and authorized before distribution, in the same way as a letter written on school headed paper.

Photos and videos – All parents must sign a photo/video release slip when their child joins the school; non-return of the permission slip will be assumed as acceptance. Photos or videos taken on a device for curriculum purposes must be transferred to our school's network and then removed the same day. A device which is being used during residential trips must be kept in a secure area and photos and videos downloaded at the end of the trip.

System – Encrypted USB storage devices for staff can be used for transferring documents containing pupil's personal information, including photos and videos. School laptops and documentation stored on the system drives will be monitored by IT Support. Staff shall not use any personal device (e.g. personal cameras/phones) to store pupil information including photos/videos. Student drives will be monitored and pupils may bring in personal storage devices as a means of transferring homework but must be given to IT Support for virus checking.

Website - The contact details on the website are the school's address, e-mail and telephone number. Staff or pupils' personal information shall not be published. The Headteacher or nominee shall take overall editorial responsibility and ensure that content is accurate and appropriate. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupils' full names shall not be used anywhere on the website including in blogs, forums or wikis, particularly in association with photographs. All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use.

Notice and take down policy – Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Social Networking – there are many social networking services available, however Herne do not permit the use of any external social media site in school unless short-term access is required for a specific educational project. This does not include blogs, wikis or forums accessed via any online platform. Content/comments posted on these sites shall be monitored by the school staff and IT Support. Access to social media sites are filtered by HCC, however if access is required, a request should be sent to IT Support who will liaise with HCC accordingly. Herne has an official Twitter and Facebook account which is only updated and monitored by the Head Teacher or IT Support.

Note: Herne believes our pupils should adhere to the age of consent rules when opening a social media account (users should be a minimum of 13 years of age) and teaching of these rules will be given in Online-Safety lessons.

School staff must take care to protect their privacy and protect themselves from risk of allegations in relation to inappropriate relationships and cyberbullying. Staff must not have any unauthorised contact or accept 'friend' requests through social media with any pupil (including former pupils and/or those who attend other schools) unless they are family members. If employed by the school, it is crucial to refrain from referring to school matters, whether this is regarding information about a child, another member of the Herne team or, in the case of staff who are also parents of the school, their experiences of the school as a parent. Staff must exercise caution when having contact online through social media with parents so as not to compromise the school's reputation or school information. This includes staff contacting other staff in any sort of public domain which can be seen by other members of the public (e.g. parents or children).

The following good practices shall be performed in accordance with the GDPR framework:
All staff to:

- Lock their computer screens when leaving their desk
- Be mindful of conversations you have around school - who else is in ear shot?
- Class cameras/school iPads to be used when taking photographs of pupils
- If leaving a voicemail try not to name the child
- Securely store all data (documents etc.) when you are not using them
- Make use of the Remote Desktop connection facility to log onto schools drives from home. Alternatively, encrypted memory sticks to be used.
- Ensure all pupil work, which is taken home, is transported in boot of the car and kept safely.

Mobile technologies - Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. They often provide a collaborative working environment and thus open to risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

- The school allows staff to bring in personal mobile phones and devices for their own use. The school does not allow a member of staff to contact a pupil or parent/carer using their own personal device, unless under exceptional circumstances and with prior agreement from the Senior Leadership Team.
- Pupils are allowed to bring personal mobile devices / phones to school but they must be switched off whilst in school. They must be kept securely and out of sight and should be stored in the class locker. Smart watches brought to school must be disconnected from the internet. We reserve the right to place them in the class locker if they distract pupils during lessons. The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Herne have the use of Google Workspace, which is a cloud based solution, enabling pupils to access school work from their Outlook Account via any internet enabled device. Pupils have the ability to 'share' their work only with staff and pupils within the school community. Activity shall be monitored by IT Support and pupils are reminded of the rules on respectful collaborative learning at the start of the lesson.

Incidents & Complaints – Any Online-Safety incident is to be brought to the immediate attention of the Headteacher or in their absence, the Online-Safety Coordinator(s). The Headteacher will assist you in taking the appropriate action to deal with the incident and in adding the incident to CPOMS. Complaints of Internet misuse shall be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Sanctions within the school include: – interview/counselling by class teacher / Headteacher; – informing parents or carers; removal of Internet or computer access for a period.

Training and Curriculum – The Headteacher and Online-Safety Coordinators are responsible for staying up to date with new information/research pertaining to Online-Safety. Herne will have an annual programme of training which is suitable to the audience.

Online-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff shall ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Teaching and Learning

Children shall be taught about Internet safety using materials from Project Evolve and in accordance with the Computing curriculum. This will take place within Computing and PSHE lessons.

Pupils shall be informed that network and Internet use is monitored. Online-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

Staff may only create blogs, wikis or forums in order to communicate with pupils using the school's website or other systems approved by the Headteacher.

Pupils shall be supervised at all times when using the internet. They are given clear objectives and must ask permission before accessing different sites. All websites used in lessons, are checked by staff.

Prompt action shall be taken if pupils encounter inappropriate material. Both staff and pupils are taught to switch off the monitor and pupils must report the incident immediately to a member of staff. Staff must record the website address and report it to the IT Support, Online-Safety Coordinator or Headteacher, whom must then report it to HCC (as above). If necessary, a discussion will take place with the pupil and parents/carers shall be informed.
Pupils shall be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Important aspects surrounding the laws on copyright of material will also be covered.

Pupils shall be taught:

- The importance of Digital Citizenship (respect, courtesy and responsibility) when communicating with others online.
- Never to give out personal details of any kind which may identify them or their location (i.e. full name, address, mobile/home phone numbers, school details, IM/email address, and specific hobbies/interests).
- To deny access to unknown individuals and how to block unwanted communications. Students are told to invite known friends only and deny access to others.
- The importance of passwords and other levels of security such as Anti-Virus & Malware protection.
- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy. In addition, pupils will be taught about the importance of copyright laws and illegal use of information from the internet.
- Not to place personal photos on any social network space provided in the school learning platform.
- The use of social network spaces outside school is inappropriate for primary aged pupils, parents / carers will also be advised.
- Not to share passwords or use another's account on any digital system. Staff shall model this behaviour by only using their own school accounts whenever possible.
- To be cautious about the information given by others on sites, for example users not being who they say they are.
- To avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- To set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- To be wary about publishing specific and detailed private thoughts online.
- To report any incidents of bullying to the school.
- Clear guidance on how to seek help and support if they experience an incident on the internet

Links and Information

Further information can be found from the following sources:

- The Think u Know website by Child Exploitation and Online Protection (CEOP) website
  www.thinkuknow.co.uk/parents or www.thinkuknow.co.uk/teachers
- Use www.pegi.com to check suitability for all games (E.g. PlayStation, Wii, Xbox etc)
- NSPCC - www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- Childnet - http://www.childnet.com/
- Google's informative safety center has a simple step by step guide:
  www.google.com/familysafety/tools

Annexes have been added to this policy:

Annex A – (Attached to this document) Online-Safety Audit Template
Annex B – The Computer Charter

Policy monitored by IT Support, Headteacher, Online-Safety Coordinators.

Written: January 2024
Review date: January 2025

Related documents

Acceptable use of ICT Policy (for Staff, Governors and Visitors)
Acceptable use of ICT Policy (Pupils)

Online-Safety Audit

This quick audit will help the senior leadership team assess whether the basis of online-safety are in place to support a range of activities.

The school has an online-safety policy	Y/N
Date of latest update:	
The policy was agreed by governors on:	
The policy is available for staff	Y/N
And for parents	Y/N
The designated Child Protection Coordinator is	
The Online-Safety Coordinator is	
How is online-safety training provided?	
All staff sign an Acceptable ICT Use Agreement.	Y/N
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	Y/N
Rules for Responsible Use have been set for students.	Y/N
These rules are displayed in ICT suite.	Y/N
Internet access is provided by an approved educational Internet service provider and complies with requirements for safe and secure access.	Y/N
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y/N
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures are supervised by a member of the senior leadership team.	Y/N
An ICT security audit has been initiated by the senior leadership team, possible external expertise.	Y/N
Staff are aware of Think U Know training (CEOP website).	Y/N
The school filtering policy has been approved by the senior leadership team.	Y/N