HORLEY INFANT SCHOOL

E-SAFETY POLICY
(including acceptable use of photo/video)

Initially Approved On: Autumn 2003
Reviewed On: Autumn 2018
Staff Link: Anusha Doolly
Link Governor (statutory policies only): Fiona Stimpson

Next Review Date: Autumn 2019
FGB Review (statutory policies only): Resources
Horley Infant School E-Safety Policy

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation; technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school in their use of technology and establishes mechanism to identify, intervene in and escalate any incident where appropriate (Keeping Children Safe in Education).

Writing and reviewing the E-safety policy

The E-safety Policy is part of the School Development Plan and relates to other policies including those for Teaching and Learning, Curriculum Anti-bullying and for Child protection and safeguarding.

Anusha Doolly is the E-safety Co-ordinator.

Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.

The E-safety Policy and its implementation will be reviewed annually alongside the Child Protection and Safeguarding Policy.

Teaching and Learning

Internet use is a supportive tool in delivering Computing, which is a part of the statutory curriculum. The internet access is provided by Virgin. Smoothwall provides the filtering contract.

Internet use enhances learning

- Pupils are taught what internet use is acceptable and what is not and given clear objectives.
- Pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieving and evaluating information.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright laws.
- Pupils should be taught to be aware of the accuracy of the materials they read. They will be shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content.

Managing Internet Access

Systems Security

- The schools’ anti-virus system is updated daily and managed centrally on the server. When a laptop is switched on, it updates. We use Sophos Anti-Virus.
- The schools’ anti-virus system is managed centrally and viewed weekly. Virus notifications are highlighted if a laptop is infected and the user is notified.

E-mail

- Staff may only use the approved e-mail accounts on the school system.
- In-coming e-mails should be treated as suspicious and attachments not opened unless the author is known.
Publishing content on the school website
- The contact details on the website should be the school address, e-mail and telephone number. Staff and pupils personal information will not be published.
- The head teacher and named member of staff will take overall editorial responsibility and ensure that the content is accurate and appropriate.

Publishing pupils' images and work
- Individual photographs that include pupils will never contain the child's name or class details.
- Pupils’ full names will not be published on the school website.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website (permission will be obtained as part of the induction process). This information is available from the School Office and all teachers to have a copy in their classrooms.

Filters and monitoring internet use in school (Keeping Children Safe in Education)
- The school uses Smoothwall, Firewall and Web-filtering to ensure the school network and systems protect pupils from incoming and outgoing internet activity.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety/Computing co-ordinator (see reporting unsuitable material form).
- Filtering systems are in place to ensure the school is doing all they reasonably can to limit children’s exposure to child sexual exploitation; radicalisation and sexual predation and other issues surrounding safeguarding.
- All staff with access to the internet and shared systems in school login via an individual username and password, this means all internet activity is filtered, monitored and recorded.
- Pupils do not have individual usernames and passwords therefore we cannot monitor pupils. Laptops all have identification names which are filtered and monitored. This coupled with a timetable of groups using laptops would enable the school to locate any inappropriate use to groups of users if an issue should arise.
- The computing technician ensures that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Weekly checks regarding suspicious internet activity, including web-search phrases for all user groups are carried out, analysed and a report log completed.

Monitoring Strategies
The school will use the following strategies to monitor internet use:

<table>
<thead>
<tr>
<th>Type of Monitoring</th>
<th>A brief explanation of the monitoring strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical monitoring</td>
<td>Where staff directly supervise children using technology and monitor screen activity</td>
</tr>
<tr>
<td>Internet and Web access monitoring</td>
<td>Filtering provides log-file information that details and attributes websites access and search terms usage against individuals and groups.</td>
</tr>
<tr>
<td>Monitoring Content</td>
<td>Recognising that no monitoring can guarantee to be 100% effective, schools should be satisfied that their monitoring system covers the following content/keywords: Illegal, bullying, child sexual exploitation, discrimination, drug/substance abuse, extremism, pornography, self-harm, violence and suicide.</td>
</tr>
</tbody>
</table>
Managing emerging technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Games machines that have internet access which may not be filtered will be used with care within the school.
- Mobile phones and associated cameras will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. (Refer to Page 7 for more details)
- The appropriate use of learning platforms e.g. Purple Mash and Bug Club will be discussed as the technology becomes available within the school.

Protecting Personal Data
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet Access
- All staff are granted access to the school’s computing systems.
- All (pupils’) internet access will be adult demonstrated with directly supervised access to specific, approved online material.
- Parents will be asked to sign and return a consent form (see Code of Conduct).
- Any person not directly employed by the school will be asked to sign an ‘acceptable use of school computing resources’ before being allowed to access the internet from the school site.

Assessing Risks
- The school will take all reasonable precautions to prevent access to inappropriate materials. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed.
- The school will review Computing annually to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints
- Complaints of internet misuse will be dealt with by the head teacher.
- Any complaints about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt within accordance with school child protection procedures.
- Pupils and parents will be informed of pupils misusing the internet. Consequences for misuse will be age and time appropriate to the pupil involved e.g. suspension from all devices/laptops in school for a week.

Community use of the Internet
- All use of the internet connection by the community and other organisations shall be in accordance with the e-safety policy.

Communications Policy
- Appropriate elements of the e-safety policy will be shared with pupils.
- E-safety rules will be posted in all classrooms and on each individual laptop/computer.
- Pupils will be informed that internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils through computing lessons and PSHE.

Staff and the e-safety policy
• All staff will be given the school e-safety policy and its importance explained.
• Staff will be aware of/carry out data handling guidance set outline by Becta and Surrey County Council.
• Teaching staff will be asked to sign and return a code of conduct (see teacher code of conduct).

Social media
• Staff and pupils working in the school are only expected to communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner. All staff and pupils working in school have agreed to conduct their activity on social networking sites with the highest of professionalism. It has been agreed that:
  ✓ No inappropriate photographs, status updates or conversations will be uploaded.
  ✓ No member of staff/pupil will be linked on-line to parents of pupils in school.
  ✓ No member of staff/pupil will be linked on-line with pupils.
  ✓ Staff/pupils will not comment on school related issues, nor engage in school related conversations.
  ✓ Staff/Governors/pupils will not up-load photographs or images of colleagues, pupils or any school related business.

Photographs
• All teaching staff are issued with a school camera and SD (secure digital) card. It has been agreed that staff will not use personal SD cards to take pictures and store images of pupils.
• Under no circumstances should mobile phones be used to take photographs of pupils or other photographs in school.

Mobile Phones
• Staff and pupils working in school will ensure that mobile phones are switched off or turned to silent mode during lessons (ensuring phones do not ring/vibrate). Staff and pupils should never use mobile phones for making/receiving calls and sending/receiving text messages and emails when children are present. Staff and pupils need to use their professional judgement to determine if it is appropriate to make/receive calls and send/receive messages at lunchtime and after school, taking into consideration their location in school and the presence of children. Staff and pupils have been asked not to walk through school talking on mobile phones and to keep mobiles out of sight of children (for example, not left on desks in the classroom).

  • Continued vigilance in school is important; everyone is responsible for the safe guarding of children and must ensure mobile phones are used in-line with this policy (everyone is accountable; if you see someone using a mobile phone which breeches the policy, this needs to be challenged).

  • If the agreed codes above are broken, action will be taken in-line with the school’s disciplinary policy. The same applies to trainee teachers and pupils as well as being reported to their university and/or college/school.

Enlisting parents’ support
• Parents’ and carers’ attention will be drawn to the school e-safety policy in newsletters, the school brochure and on the school web site.
• Parents and carers will from time to time be provided with additional information on e-safety.
• The school will ask all new parents to sign the parent code of conduct as part of the induction process.
Parents taking photographs and videos

- Education staff are often asked by parents/carers whether they can make video recordings or take photographs of their children at school events such as nativity plays and sports days. This guidance has been developed to support education settings to allow this to occur while ensuring that all young people who may be photographed or videoed are safeguarded.

- Photographs and videos of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. Therefore, using such photographs for school publicity purposes requires the consent of either the individual concerned or in the case of pupils, their legal guardians.

- However, parents/carers are not required to comply with the terms of the Data Protection Act when taking photographs or video of their children for their own personal use at an organised event. It is lawful and can be allowed. Parent/carers should, nonetheless, be made aware that the use of the photographs/video must be strictly for personal use and should not be shared online (i.e. through any social media network), sold nor distributed via any other means.

- Education settings reserve the right to decide whether they wish to allow parents/carers to take photographs/video at events. The setting also reserves the right to withdraw the consent for parents/carers to take photographs/video for example on health and safety grounds (i.e. due to excessive use of flashlights or bulky and noisy equipment which could also be distracting for pupils).

- In light of emerging mobile technology and the ease of uploading photographs onto social media sites, it has been agreed that parents may take photographs at class assemblies and similar school events. However, parents will be asked to use photographs for personal use only and not to upload onto social media sites. A message will be given out at every class assembly or similar event.

- Parents taking photographs at school events will be reviewed in-line with the annual e-safety review or sooner if the school feels that photographs are not being used appropriately (i.e. being up-loaded onto social media sites).

- Horley Infant School reserves the right to ask a parent/carer to leave if they are observed taking inappropriate photographs/video or if they are observed covertly using photographic/video equipment. Where this occurs Horley Infant School will follow necessary safeguarding procedure.

- Horley Infant School reserves the right to remove consent to take photographs/video at any time.

- Parents/carers are required to follow additional guidance in event programmes or announcements from school staff as to when photography and videoing are permitted.

Parents using mobile phones

- Whilst it is recognised that mobile phones are an important part of modern life; parents have been asked not to use mobile phones in school for making and answering calls, sending and receiving messages.

- Parents helping on Educational/school trips must not use their mobile phone during the course of the day for making and receiving phone calls, sending messages and emails, accessing social media sites or taking photographs. It is the responsibility of the teaching staff leading the trip to ensure that parents are aware of this policy and the information is communicated to parent helpers both verbally, during the briefing, and in writing within the parent helper booklet.
Mobile Device Guidance
General use of mobile phones/personal devices

- Mobile phones and personally owned devices will not be used in any way during school hours. This includes lessons or any activity during formal school time. They should be kept in bags and switched off or on ‘silent’ mode at all times.
- The Bluetooth functionality of a mobile phone should be switched off at all times and not be used to send images or files to another mobile phone.
- Mobile phones and personally owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.

Pupil’s use of mobile phones/personal devices

- Due to the very young age of our current pupils there is no circumstance when they would need to bring a mobile phone or personal device into school.
- If for any reason a pupil brings a mobile phone or personal device into school, it will be taken into safekeeping by a member of staff and parents informed.
- This guidance will be reviewed annually to take into account the changing circumstances as the school grows.
- It is not considered necessary to have an Acceptable Use Agreement for pupils at this time.