Havelock Schools E-Safety and Acceptable Use Policy

Why do we have an e-safety Policy?

We believe that the internet is an essential part of 21st century life and has a valuable role to play in the education of our pupils. Our school has a duty to provide our pupils with quality internet access as part of their learning experience. The use of the internet is part of Havelock Schools' Scheme of Work for computing and the internet is a useful resource that enhances the teaching and learning taking place within our school. In delivering the curriculum, teachers need to plan for and make use of communications technology, for example, web-based resources and e-mail. Access to life-long learning and employment both increasingly require computer and communications use and pupils need to develop computing life skills. Home and social internet use is expanding and it is becoming an important part of learning and communication during leisure time. This brings pupils into contact with a wider range of information, the scope and nature of which may, or may not be appropriate for the pupil. There are also wider dangers that e-mail and chat, telephone conversations and text messages, could all be used as a means of anonymous communication with pupils by adults with inappropriate intentions. **Whilst we are an Infant/Junior school our pupils use the internet and ICT on a daily basis and we believe that their e-safety education should start as soon as technologies are introduced.** Our aims as a school and with this policy are to ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies, to outline the roles and responsibilities of everyone. To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting and to develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

As a school we recognise that e-safety encompasses internet technologies and electronic communications, such as mobile phones as well as collaboration tools and personal publishing, which is why we have an e-Policy rather than an internet Safety Policy. We also recognise that e-safety highlights the need to educate pupils about the benefits and risks of using technology as well as our responsibility to provide safeguards. We need to make all users aware of e-safety and help them to control their online experience. All teachers using ICT in the classroom have a duty to ensure that pupils are reminded about appropriate behaviour regularly.

We believe that the internet is a valuable teaching resource that can enhance learning and raise educational standards by offering pupils and teachers opportunities to search for, and access multimedia information from a range of sources all over the world. We understand that as with any school resource ICT needs to be managed carefully to ensure its educational effectiveness and safe usage.

Our school is aware that some of the information on the internet is inappropriate for our pupils and that we need to have an e-safety policy which is understood by and adhered to by all members of staff, including individuals working in a voluntary capacity. This policy defines the appropriate and acceptable use of the internet by both staff and pupils.

Legal Background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within the following legislative documents which should be referred to for further information:

- The Children Act 2004
- School Staffing (England) Regulations 2009
- Working Together to Safeguard Children 2010
- Education Act 2002
- Safeguarding Vulnerable Groups Act 2009

All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy includes, but is not restricted to the legislation listed above.

Roles and Responsibilities

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Safeguarding) across the school. The Designated Safeguarding Lead takes responsibility for managing e-safety within our school working in conjunction with the Computing subject leader and the internet administrator. The e-safety policy and its implementation will be reviewed annually and the school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective. The school's Computing systems capacity and security is managed by NuIsolutions. ICT Staff will ensure that virus protection is updated regularly and take responsibility for Firewall and antivirus software. The ICT Technician is responsible for the virus protection on laptops. The provision of Broadband internet access and wireless connectivity is organised and managed by NuIsolutions.

E-Safety Education

We will continue to ensure that the school's internet access will be designed for our pupils' use and will include filtering appropriate to the age of pupils. E-safety lessons will form a regular part of the children's education both within the discrete teaching of Computing and when the internet is used across the curriculum. Our pupils will be taught when internet use is allowed; what internet use is acceptable and will be given clear learning objectives related to internet use. The children will be taught rules that will help to protect them when using the internet both at school and at home. We will also provide parents with information about e-safety through newsletters, the school website and included in our School Prospectus will be the E-safety rules. Parents are invited in to the school to join their children in learning about E safety. Assemblies are held termly to highlight the importance of E-Safety to all. All adults working in the school will be aware of the CEOP Report Abuse button (www.thinkuknow.co.uk) as a place where they can make confidential reports about online abuse, sexual requests or other misuse as well as a place to find age appropriate resources to help teach e-safety. The CEOP button is on both the Infant and Junior school websites to help report any issues. The NSPCC Whistleblowing support line is available for staff who do not feel able to raise concerns regarding child protection failures internally or feel that their concerns have not been listened to:

NSPCC Whistleblowing support line

Staff can call: 0800 028 0285 – line is available from 8:00 AM to 8:00 PM, Monday to Friday and Email: help@nspcc.org.uk.9

Our Pupils

Pupils will only be allowed to use the internet when supervised by teaching staff and teaching assistants and when asked to do so. Pupils may log on to the internet using their own logins and passwords or the generic year group login. These are allocated to individual pupils'. Pupils will only use email when supervised by adults and when instructed to do so. Junk Mail is filtered out to ensure that the accounts have not received any offensive or inappropriate emails. Pupils will be taught not to reveal any personal details of themselves or others in online or phone communications, or arrange to meet anyone without specific permission. If staff suspect a child is using social media under the age restriction, this will be reported to the DSL.

The School Website

The point of contact on the Web site is the school address, Headteacher's e-mail address and the school telephone number. Staff or pupils' home information will not be published. We want our school web site to reflect the diversity of activities, individuals and education that takes place at Havelock Schools. However, the school recognises the potential for abuse that material published on the internet may attract, no matter how small this risk may be. Photographs of children can only be published to the website with the parents' written permission. (Records of which parents have not given consent can be found in the class registers). Pupils' full names will not be used anywhere on the website, particularly associated with photographs. The Headteacher and Web Administrator will take overall editorial responsibility and ensure content is accurate and appropriate.

Filtering

The school will ensure that filtering of websites is done appropriately. This is managed by NuI Solutions. If staff or pupils discover an unsuitable site, it must be reported to the e-safety Coordinator. The E-safety co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Use of School Equipment

School equipment must remain on school premises, with the exception of school laptops unless permission is given. However no material of a personal nature should be stored on these laptops i.e. photographs of children or children's personal details including email addresses. All such material should be stored on the school shared drive or school computers only. All staff will be issued with a school memory stick which should only contain material for school use and should not include any personal information or photos.

Use of Personal Equipment

Use of personal cameras, mobile phone cameras or recorders, Dictaphones, MP3 players, and memory sticks are not permitted in school. Only school equipment should be used to take photos or videos of children and these should not be taken home by anyone. Use of mobile phones during class time is not permitted. School mobiles must be used during a school trip also.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in accordance with the school's Confidentiality Policy.

Acceptable Use

All staff must read and sign this e-safety and Acceptable Use Policy before using any school ICT resource. The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn. Users are managed by the internet Administrator in accordance with the e-safety Coordinator.

All internet activity should be appropriate to staff professional activities or the children's education. Access to the internet within school is limited to the use of authorised accounts and passwords, which should not be made available to any other person. Each member of staff has their own internet login details which should be kept private. There is a separate logon for each individual within school. Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited. Staff are not permitted to use their own personal email accounts for work purposes. In regards to e-mail, users are responsible for all e-mails sent and for contacts made that may result in e-mails being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media. All web activity is monitored, including the content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task.

Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon may be in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights.

At Havelock Infant/Junior School initial access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NuIsolutions can accept liability for the material accessed, or any consequences of internet access.

Children must not be given unsupervised access to the internet. For the purposes of this policy, "supervised" means that the user is within direct sight of a responsible adult. The teaching of internet safety is included in the school's planning, but all

teachers within all year groups should be including internet safety issues as part of their discussions on the responsible use of the school's computer systems. All of the pupils should be regularly reminded of the School's internet Rules. All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.

Complaints of internet misuse by children will 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. Pupils and parents will be informed of the complaints procedure.

There is not currently any unsupervised community use of the internet within school. Stay and Learn sessions run for parents and children with access to computers and are monitored by a member of staff. Should the school's internet facilities be used by community groups in the future the e-safety policy would need to be amended to include those parties and their adherence to the policy would need to be agreed before any use could commence.

E-safety rules (see appendix) will be given to each member of staff, displayed in each classroom, displayed on the side of the laptop trolley, included in the school prospectus and posted on the website. The children will be taught e-safety rules during discrete computing subject teaching and when the internet is used across the curriculum. Pupils will be informed that network and internet use will be monitored.

All staff will be given the school e-safety policy and the importance of the policy will be clearly explained. The e-safety policy will be available on the school website for both teachers and parents to access. All staff should be aware that internet traffic can be monitored by the service provider and can be traced to the individual user. Discretion and professional conduct is essential.

Parents' attention will be drawn to the School e-safety Policy in newsletters, the school prospectus and on the school Website. We hope that taking an active role in providing parents with information and guidance about e-safety we will further protect our pupils and help to ensure that they are getting e-safety messages in the home too. We realise that parents and carers have a key role in promoting e-safety at home. Computing offers the opportunity for children and parents to learn together and e-safety is a topic which can be taught at home and school.

Any images or videos that are deemed unsuitable by staff (due to the content) will be reported to the DSL, even if the images or video were taken and/or circulated by the child themselves.

Useful Links

CEOP (Child Exploitation and Online Protection)
www.thinkyouknow.co.uk

NASUWT Social Networking- Guidelines for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking

NUT E-Safety: Protecting School Staff- Guidance for Members
http://www.teachers.org.uk/node/12516

UNISON- Guidance on Social Networking
http://www.unison.org.uk/education/schools/pages_view.asp?did=9786

Date to be reviewed November 2017

Also see the following policies: Anti-bullying, Complaints, Social Media, Physical Intervention, Behaviour, Child Protection, Whistleblowing, Code of Conduct

Appendix 1

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any online technologies, such as the internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.

- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed……..Date……..
Name (printed)…….
School……...

Appendix 2

Staff Procedures for Misuse

These procedures should be followed in the event of any misuse of the internet:

A. An inappropriate website is accessed inadvertently:
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and NuIsolutions so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Report to the Headteacher and e-Safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform NuIsolutions filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Headteacher immediately.
Ensure the device is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Headteacher and Designated People for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, NSCBN.

Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated People for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:
Preserve any evidence.
Inform the Headteacher immediately and follow Child Protection Policy as necessary.
Inform the RBC/LA/NSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance.
All adults should know who the Designated People for Child Protection are.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix 3

Children and Young People's Procedures for Misuse

These procedures should be followed in the event of any misuse of the internet:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and MCLP/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform NuIsolutions as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Headteacher and Designated People for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence.
Inform the Headteacher immediately.
Inform the NuIsolutions/LSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

Appendix 4

Havelock Junior School's E-Safety Rules for Pupils

Havelock Junior School pupils keep to these rules and know how to stay safe when using computers

E-SAFETY RULES:

- Keep passwords safe and secure – do not share them with anyone.
- Only use activities that a teacher has told or allowed me to use.
- Take care of the computer/iPad and other equipment.
- Do not share personal information about yourself when online.

- Do not take or distribute images of anyone without their permission.
- Do not install or attempt to install software of any type on a device or on a computer.
- Do not alter or try to computer/device settings.
- Tell a teacher if you see something that upsets you on the screen.

Date/time of Incident:
Child and/or Workstation/Device name including reports from outside school:
Incident or concern raised:
What actions were taken, by whom and why?
Other information:
Has any computer or hardware been secured? If so, how/where?

Has the information been recorded and secured? If so, how/where?	
Member of staff reporting concern:	**Signed:**
Online Safety Coordinator/Designated Safeguarding Lead:	**Signed:**
Action taken by Online Safety Coordinator/Designated Safeguarding Lead:	

Appendix 5

Havelock Schools Online Safety Incident Reporting Form

Havelock Infant School's rules for using the internet.

 We only use the internet when an adult is with us. We only use websites our teachers have chosen.

 We only click on buttons and links when we know what they are.

 We only use search engines designed for children and always use them when an adult is with us.

 We always say when we get lost on the internet. If we see something that upsets us we tell an adult straight away. We close websites immediately we don't like.