The Heights Primary School Policy for

E-Safety

Version 1.0

Responsible officer:	Headteacher
Responsible Committee:	Pupil and Staff Welfare Committee
Date of last review:	February 2017
Date of next review:	February 2018

Introduction

At The Heights Primary School, we understand the responsibility to educate our pupils on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

ICT in the 21st Century is seen as an essential resource to support leaning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

1.0 Effective Practice

E-safety depends on effective practice in several areas.

- Education for responsible ICT use by staff and pupils.
- A comprehensive, agreed and implemented e-safety policy.
- Secure filtered internet access in school.
- A school-wide commitment to ensure safe practice by all who work with children.

1.1 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 ICT, bullying and for child protection.

- The school has an e-Safety Coordinator. This is the Designated Safeguarding Lead. It is not a technical role.

1.2 Teaching and learning

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught to report unpleasant internet content to a member of staff.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.

1.3 Managing Internet Access

Information systems security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- The school will pay due care and attention to advice on improved IT Security offered by external agencies, such as the DfE, Local Authority or appointed ICT Consultant.
- Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Accesing the Wi-Fi network

- The Heights Primary School currently operates two distinct Wi-fi networks with separate SIDs. There is a staff network and a visitor network. The staff network is for all school devices such as iPADs or teacher laptops to connect to and is filtered. The network uses WPS2 security so access is password protected.
- The second Wi-Fi network is for visitors to the school such as visiting teachers, invited speakers or specialists such as school nurses, educational psychologists etc. The visitor network is not filtered it also used WPS2 security and is password protected. The password to this network will be changed on a regular basis.
- Any visitor to the school who wishes to make use of the visitor Wi-Fi network will need to sign the fair usage agreement attached to this policy.

Managing filtering

- The school will work with outside agencies, as mentioned above, to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- If videoconferencing is to be attempted it should be done making use of a device with a cabled Ethernet connection, not by using a device attached to the WiFi network. This is to ensure the best quality of service and security of the connection.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Streaming Internet Content

- Video and music content from authorized sites may be used providing the staff member accessing the content ensures that due regard is taken to copyright or licensing restrictions and that the material is ag-appropriate.
- In order to protect the school's data allowance any staff member accessing streamed content must close the browser session used to access the content once viewing or listening is complete. This is to ensure that the streaming session is closed down and dos not inadvertently run overnight or for an extend period of time.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school's web site.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both

on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Ideally pupils would use only moderated social networking sites, e.g. Think.com
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- School will act in accordance with child protection procedures and notify parents if any child is known to use these sites or is accessing software that is not of an appropriate age for the child eg games such as Black Ops and C.O.D.

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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time by anyone on the school premises. Children's mobile phones will be left in the office for the duration of the school day unless other specific arrangements have been made with the agreement of the Headteacher. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others are not permitted on school premises.
- During offsite activities staff may need to use a mobile phone to communicate with appropriate adults. Mobile phones may not be used to capture or record images (unless exceptional circumstances apply and with the agreement of the Head teacher.

Protecting personal data

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

1.4 Policy Decisions

Authorising Internet access

- All staff, Governors and visitors must read and sign the Acceptable Use Agreement before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return an acceptable use agreement on behalf of their child.
- Any person not directly employed by the school will be asked to sign the Acceptable Use Agreement before being allowed to access any ICT resource with an internet connection, including the school's WiFi network, as mentioned above.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use 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 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's safeguarding policy.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- The local police will be informed of potentially illegal issues.
- Inappropriate use of a school computer will result in disciplinary action.

1.5 Communication of this Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-safety will be developed, possibly based on the materials from CEOP.
- E-safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.
- E-Safety training will be made available to all staff via the Educare online training platform. Governors may also choose to access this training.

Staff and the e-Safety policy

- All staff will be given the school e-safety Policy and its importance will be explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- Communication with pupils by email must be through school approved email addresses
- Staff are advised that social networking sites may pose a threat to professional roles if care is not taken to protect privacy. (Some teaching unions (E.g. NUT) advise members not to use social networking sites.)
- No current or past pupil should be added as a ‘friend’ on any social networking site.
- We expect all staff to be good ambassadors for The Heights Primary School and to do nothing that would undermine our good standing in the local community or bring the school into disrepute. Staff should be aware of this when posting comments on public forums.

Enlisting parents’ and carers’ 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.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the ICT agreement when they register their child with the school.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant resources
Using web directories and bookmarks to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks, Google Chrome
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	SuperClubs Plus Global School Net Global Kids
Publishing pupils work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils full names and other personal information should be omitted. Pupils' work should only be published on moderated sites and by the school administrator.	Making the News SuperClubs Plus Headline History National Education Network
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing

Appendix 2: Useful resources for teachers

BBC Stay Safe www.bbc.co.uk/cbbc/help/safesurfing/

Becta http://schools.becta.org.uk/index.php?section=is

Chat Danger www.chatdanger.com/

Child Exploitation and Online Protection Centre www.ceop.gov.uk/

Childnet www.childnet-int.org/

Cyber Café http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen www.digizen.org/

Kidsmart www.kidsmart.org.uk/

Thames Valley Police Online Safety Advice: http://www.thamesvalley.police.uk/crime-prevention/keeping-safe/online-safety.htm

The Prevent duty https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Think U Know www.thinkuknow.co.uk/

Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Care for the family www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD http://publications.teachernet.gov.uk

Family Online Safe Institute www.fosi.org

Internet Watch Foundation www.iwf.org.uk

Parents Centre www.parentscentre.gov.uk

Internet Safety Zone www.internetsafetyzone.com

Appendix 4: E-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head teacher.

Has the school an e-Safety Policy that complies with LA guidance?	Y/N
Date of latest update (at least annual):	
The school e-safety policy was agreed by governors on:	
The policy is available for staff at: The Heights Primary School website	
The policy is available for parents/carers at: **The Heights Primary School website**	
The responsible member of the Senior Leadership Team is: **Karen Edwards**	
The responsible member of the Governing Body is: **Chair of Governors**	
The Designated Safeguarding Lead is: **Karen Edwards**	
The e-Safety Coordinator is: **Karen Edwards**	
Has e-safety training been provided for both pupils and staff?	Y/N
Is there a clear procedure for a response to an incident of concern?	Y/N
Have e-safety materials from CEOP and Becta been obtained?	Y/N
Do all staff sign a Code of Conduct for ICT on appointment?	Y/N
Are all pupils aware of the School's e-Safety Rules?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DFE requirements?	Y/N
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	Y/N

Appendix 5: The Heights Primary School E-Safety Policy
iPad Acceptable Use Policy

The Heights Primary School has purchased iPads for cross-curricular learning. We believe our iPads will enhance the way our pupils learn by offering them personalised access to creative ICT tools and new ways of learning. As with all emerging technology we recognise there are likely to be 'unknown factors' and when they make use of the internet in such an innovative way, where technology is rapidly changing, keeping our learners safe is paramount. Therefore, this iPad acceptable use policy should be read alongside our general e-safety policy on the understanding that it will be regularly updated as we become aware of additional e-safety issues. At no time can the school or its representatives be held liable for any losses or omissions as a consequence of following this policy.

General Use

- Users must use the protective cases / covers provided with the iPad
- When not being used iPads should be stored in the designated place
- iPads should only be charged when 10% of battery life is remaining, to conserve battery life
- Only soft cloths or approved cleaning solution should be used to clean the iPad screen
- iPads should be kept away from food, drink and other liquids
- iPads should not be subjected to extreme temperatures
- All reasonable care should be taken when iPads are used around the school, so as to avoid
- accidents
- Care should be taken to avoid dropping or bumping the iPad as this will damage or break the
- screen
- Items such as pens, books, learning equipment and heavy objects should not be placed on top of an iPad as this may crack or break the screen
- Users of iPads should follow a clean hands policy
- Malfunctions and damage to an iPad should be reported immediately to the School Business Manager
- When iPads are timetabled, pupils should use the same iPad and a record kept
- Users should be aware that iPads will be monitored and checked regularly
- Any breach of this policy or the school e-safety policy may result in disciplinary action and access to iPads revoked
- Use of the camera and microphone features are only permissable for learning and teaching
- purposes and then only with permission of the teacher
- Photographs of staff or pupils may only be taken if permission has been given
- The camera may not be used to take, copy or distribute photographs of inappropriate or illegal material in any way
- Users are not allowed to use the iPads to send, save, access, upload, download or distribute
- offensive, illegal or threatening materials
- iPads that are believed to be stolen will be tracked through iCloud and, if this is proven to be the case, reported to the police when this facility is available
- The ICT Technician / Co-ordinator will install and delete apps

- Any attempt to jailbreak the iPads (remove limitations on the iPad by Apple), destroy hardware, software or data will be subject to disciplinary procedures
- Users will not delete internet browsing history and doing so will result in disciplinary action
- Users should be aware that the iPads will be monitored regularly, including files, documents and internet browsing history - in line with our e-safety policy
- Where iPads are shared, users will not delete work or documentation belonging to another user
- Apps will only be used that are age appropriate
- Users will not access personal web accounts, such as their iTunes account or personal email, on the iPad
- iPads are for school use only and personal use will result in disciplinary procedures
- Users will not attempt to change settings on apps or in the iPad settings area - this may be different for specified staff
- Users will not attempt to log in to an iTunes account
- Wherever possible users will use an agreed file naming convention so as to easily identify documents and authors
- Confidential documents will not be accessed or created on an iPad - unless it is secure / on a teacher laptop
- Users will immediately report any offensive, illegal or threatening material found on an iPad to the ICT Co ordinator
- App updates will be managed by the ICT Technician / co-ordinator set to install automatically
- App notifications will be turned off
- Location settings may be required for some apps to be effective, each app will be assessed in its own right and a decision made according to risk
- iPads will be backed up according to school needs - on a termly basis – and work deleted ready for new term
- If users delete their own work it can only be retrieved if it was backed up on a previous occasion
- Pupils will be shown how to use the iPad before use and it will not be assumed that they know how the school systems will work. Pupils may be used to certain practices that are not appropriate in an education setting.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……..…….…… Date ……

Full Name ……..... (printed)

Job title ……

Appendix 6: Staff Professional Responsibilities

Here is a clear summary of professional responsibilities related to the use of ICT which has been endorsed by unions.
To download please visit: http://www.thegrid.org.uk/eservices/safety/policies.shtml

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

Appendix 7: Acceptable Use of ICT – Pupil

Acceptable use of ICT
Agreement / eSafety Rules

- I will only use ICT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day

The Heights Primary School
82 Gosbrook Road
Caversham
RG4 8BH
Tel: 0118 357 0123
Email: info@theheightsprimary.co.uk

For the attention of: Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school office.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂----------

Acceptable Use of ICT
Agreement / eSafety Rules

We have discussed this document with …….....(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at The Heights Primary School.

Parent/ Carer Signature ……..……..……..…….

Child's Class …… Date ……

Appendix 8 – Acceptable Use – Staff, Governors & Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet, computers and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email , internet access and any related technologies, such as a laptop, computer or tablet for professional purposes or for uses deemed acceptable by the Headteacher or Governing Body
- I will comply with the ICT system security rules and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the school's approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on Integris or in personal date used in any file or document I create) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be secured, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staffroom
- I will ensure that any computer equipment in any classroom or office that I make use of is switched off at the end of each day.
- If I step away from a computer or other device that I am using I will ensure that I lock the screen so that to protect any work that I may completing at that time and to protect my email account from malicious use.
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……..…….…… Date ……

Full Name ……..... (printed)

Job title ……