Heptonstall J, I and N School
Computing (+ e-Safety) Policy

This policy should be read in conjunction with the other policies that form part of our overall safeguarding ethos: Protecting and Safeguarding Children, Anti Bullying, Managing Allegations Against Staff, Intimate and Personal Care, Medical Conditions, Computing (+ e-Safety) and Social Networking Policies.

Introduction

The purpose of this policy is to set out the key principles expected of all members of the school community at Heptonstall Junior, Infant and Nursery School with respect to the use of ICT-based technologies, to safeguard and protect the children and staff and to set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

Computing + ICT in the 21st Century is seen as an essential resource to support learning 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 Computing + ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking (including Facebook c.f. YHGfL Guidance at Appendix 3)
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones and similar devices with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. Therefore this policy applies to the whole

school community including: Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

At Heptonstall School we understand the responsibility to educate our pupils on e-Safety 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.

Communication
The senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school Computing (+ e-Safety) Policy and the safe use of any new technology within school. We endeavour to embed Computing (+e-Safety) messages across the curriculum whenever the internet or related technologies are used.

Computing (+e-Safety) – Roles, Responsibilities and Ownership

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in this school is Peter Jenel who has been designated this role by the Governing Body. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Calderdale LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Governors are updated by the Head/e-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. Governors will contribute to and help promote the school's Computing (+e-Safety) and Social Networking policies and guidance; they will develop an overview of the benefits and risks of the internet and common technologies used by pupils.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (Appendix 1 and 2) is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

Responsibilities of Parents and Carers (+ Internet Access Authorisation)
It is the role of the parent to discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology and to model safe and responsible behaviours in their own use of technology. All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.

Responsibilities of Pupils (+ Internet Access Authorisation)
To read, understand and adhere to the school pupil Acceptable Use Policy. To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home. To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to. All pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy prior to being granted internet access within school.

Managing Digital Content

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

Publishing Pupil's Images and Work:

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:-

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Web Manager has authority to upload to the site.

Storage of Images

Any images, videos or sound clips of pupils must be stored on the school's network and never transferred to personally owned equipment.

Video Conferencing

Permission is sought from parents and carers if their children are involved in video conferences.

Learning and Teaching

We will celebrate and promote Computing (+e-Safety) through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year. We will discuss, remind or raise relevant Computing (+e-Safety) messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials. Any

internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas. Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way. We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign.

e-Safety in the Curriculum
Computing + ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise.

e-Safety Skills Development for Staff
All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community. Staff are aware that they should model safe and responsible behaviours in their own use of technology at all times.

Managing Computing + ICT Systems, Access, Passwords and Filtering

The school will be responsible for ensuring that access to the Computing + ICT systems is as safe and secure as reasonably possible. Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware, and will be kept active and up to date. All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school Computing + ICT systems and that such activity will be monitored and checked.

Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times. All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school. All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords.

The school uses a filtered internet service provided by Calderdale. The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training. The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Emerging Technologies:
Emerging technologies will be examined for educational benefit and risk assessment will be carried out before their use in school is allowed.

e-Mail and e-Mail Usage

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be

they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette ('netiquette').

Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.

Managing e-Mail

E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows: Delete all e-mails of short-term value: Organise e-mail into folders and carry out frequent house-keeping on all folders and archives. E-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.

Sending and Receiving e-Mails

Check your e-mail regularly. Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder. School e-mail is not to be used for personal advertising.

Mobile Phones and other Personal Devices

Mobile phones will not be used in any way during lessons or formal school time and should not be brought into school. If they are, pupils will be required to hand them in to reception. If a pupil needs to contact his or her parents/carers they will be allowed to use a school phone or a call may be made on their behalf. Urgent messages from parents/carers made to the school office will, of course, be passed on. In exceptional circumstances a personal or family mobile phone may be held by staff (in the office) to enable communication with a parents/carer where there is no other option. Personal devices may be allowed into school, in some special circumstances, but only with specific permission from school staff. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices that are brought into school.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personal device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- In an emergency where the staff member doesn't have access to a school owned device, they should use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

Social Networking, Blogs and other Published Content Online:
Social Networking and the use of blogs (and the publishing of any other online content) will not be used in any way during lessons or formal school time. Given the school policy on mobile phones and similar devices (see above) – there is a clear expectation that it will not be used by pupils, informally, at any other time.

Data Protection and Information Security

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information. Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.

All physical information will be stored in controlled access areas. All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted full disk, encrypted removable media. All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Breaches
A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Managing Assets

Details of all school-owned hardware will be recorded in a hardware inventory. All redundant Computing + ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Review Framework
This policy should be reviewed annually (or sooner in the event of revised legislation or guidance) and links to other school policies and statutory responsibilities.

Signed……Head Teacher Date…….

Signed……Chair of Governor Date…….

Date ratified at Full Governing Body: 9/10/2014 Review Date: October 2015

Reviewed by: Safeguarding Governor

Appendix 1

PUPIL ACCEPTABLE USE AGREEMENT AND E-SAFETY RULES

When using the school's Computing + ICT equipment and other information systems, I have understood and will comply with the following statements

- I have read and know what the computer rules in this document mean to me.
- I will only go on the internet using my own username and password.
- I will make sure that my password for the internet is difficult to guess and I will not share my password with anybody else.
- If I think someone has guessed my password I will tell a teacher.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this I will tell my teacher immediately.
- I will not try and get to any websites that the school has blocked access to.
- I will make sure I take care of any school-owned Computing + ICT equipment that I use in school or at home.
- I will only use memory sticks with permission from my teacher.
- I will not install any software on school computers.
- I will return any school-owned Computing + ICT equipment to the relevant staff member when I have finished using it.
- I know that my use of Computing + ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not damage any school-owned Computing + ICT equipment.
- I will not eat or drink while using school-owned Computing + ICT equipment.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them.
- I will not say nasty or hurtful things about any member of staff or pupil online.
- I will not give away any of my personal details (full name, age, date of birth, sex, address etc.) or the personal details of other users in school, over the internet. This includes photographs or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.

- If I see any hurtful comments about the school, staff or pupils I will report to a member of staff.

Managing Digital Content

- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Email

- I will only use my school email address to contact people agreed by my teacher.
- I will take care in opening any attachments sent by email. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- When sending emails I will make sure that they are polite and sensible. I will not use my school email account to forward chain emails.

Mobile Phones and Devices

- I will not bring my mobile phone or smart phone into school and will not take pictures, videos or make voice recordings with them in school
- I will only bring my mobile device (e.g. Nintendo DS) into school when my teacher tells me I can
- I will not take pictures, videos or other recordings in school on any mobile device.

Agreement

I agree to follow the rules set out in this Acceptable Use Agreement. I know that if I break any of these rules my parent/carer may be told.

Pupil name	
Signed	
Date	

Computing (+ e-Safety) - Parental Agreement

Dear Parent/Carer,

Computing + ICT including the use of the internet, e-mail and mobile technologies etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any Computing + ICT.

Please read and discuss this Acceptable Use Agreement (and e-Safety rules it contains) 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.

Parent/ Carer Signature

We have discussed this and ……..(child's name) agrees to follow the e-Safety rules and to support the safe use of Computing + ICT equipment at Heptonstall School.

Parent/Carer Signature ……

Full Name …….. (printed)

Class …….. Date ……

Appendix 2

Acceptable Use Agreement: Staff, Governors and Visitors

Computing + ICT (including data) and the related technologies such as e-mail, the internet 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 Computing + ICT equipment. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Peter Jenel school e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- *I will comply with the Computing + ICT system security 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 and personal e-mail address, to pupils.
- *I will only use the approved, secure e-mail system(s) for any school business.
- *I will ensure that personal data (such as data held on MIS software) 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 Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- *I will not install any hardware of software without permission of Peter Jenel
- *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 inline 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 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 support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- *I will respect copyright and intellectual property rights.
- *I will ensure that my online activity, both in school and outside school, will not bring my professional role 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 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 Computing + ICT equipment throughout the school:

Signature ……..…… Date ……

Full Name ……..…..... (printed)

Job title (or role)…….

Appendix 3

Parental Advice on Facebook

Here are some suggested guidelines on how to support your children using Facebook safely:

- The terms and conditions for Facebook state that users need to be 13 years of age. Anyone under that age who has an account is violating the terms and conditions and you can report them at http://on.fb.me/dTSqRP.

- Don't be afraid to set boundaries for your younger children and explain that, as with other forms of media, there are age restrictions on using certain websites.

- Create a Facebook account yourself and be 'friends' with your teenage children. This will enable you to monitor what they post on their wall and who they add as 'friends'.

- Facebook explicitly states that no person should abuse, harass or bully other people through posts or comments. If you come across any information that breaches this specific rule you can report it to Facebook. Guidelines on how to do this can be found at http://on.fb.me/ePpM93.

- In order to ensure that your teenage children are aware of some of the potential risks on Facebook, make sure that they download the ClickCEOP application, so that they can install the 'Report Abuse' application on their Facebook profile. Users can access this at http://apps.facebook.com/clickceop/.

- Ensure that you educate your children about their digital footprints. More colleges, universities and employers are researching candidates for jobs by searching social networking sites. A negative post or unsuitable photograph could come back and haunt your teenage children in later years and prevent them from gaining certain employment.

- Finally, teach your children to send positive posts. Schools and the police are taking seriously negative and libellous comments about educational professionals and it could lead to exclusion or legal action against them.

For further information, visit **www.yhgfl.net**