Computing and E-safety (including acceptable use of IT)

Document Control Page

Revision History

Date	Type of change	Initials	Purpose of Revision
September 2020	Major	MM	Major change to prevent use of personal devices on School IT systems and control of data extraction onto approved USB sticks only.
September 2021	Minor	MM	Change of date
January 2023	Major	JF	Amendments to out-of-date information

Headteacher signature: SBoorman

Date to be reviewed by: September 2025

Vision:

The school aims to develop independent learners who are well equipped for their future. Computing skills are an integral part of teaching and learning for pupils, staff and governors. The school believes that Computing motivates and excites pupils and enables them to achieve high standards. The school aims to use Computing to aid planning, assessment, recording and reporting and for staff to be competent and confident in this.

Supporting Policies

This policy needs to be read in conjunction with the Prevent Policy when dealing with issues relating to vulnerability, radicalisation and exposure to extreme views and the Safeguarding Policy / Child Protection Policy which includes specific guidance on radicalisation, technologies, on line safety, cyberbullying, social media, sexting, gaming, online reputation and grooming.

Aims:

Hatch Warren Infant School aims for all pupils to:

- Use their computational thinking and creativity within school and in the wider world.
- Develop Computing skills to an appropriate level and to be able to use computers safely, confidently and independently in their everyday lives, preparing pupils for the future.
- Have access to the National Curriculum programmes of study.
- Develop and broaden an understanding of the potential of Computing within their own lives and be aware of its limitations.

This can be achieved by:

- Meeting the requirements of the National curriculum as fully as possible.
- Providing a high standard Computing curriculum which motivates, challenges and involves every child, to ensure they reach the highest possible standard of achievement.
- Teaching children the skills needed to be able to use Computing equipment to manipulate and present, store and retrieve, present and enhance, interpret and analyse and to place in real life contexts.
- Providing relevant training and support for staff to ensure they can teach and support pupils effectively.

Curriculum organisation

The national curriculum for computing has four main aims to ensure that all pupils:

- Can understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation.
- Can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems.
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

The teaching of Computing will be closely linked to the other areas of the curriculum by including the Computing skills to be developed within the medium term planning for the other subjects.

All classes have a timetabled Computing session. Pupils use laptops and iPads as well as PCs located in the shared areas for each year group. In addition to this, children are able to use technology to support their learning in other curriculum areas.

In the Foundation Stage Computing is integrated throughout their curriculum.

Skills are taught through three main units of Computing:

- Computer Science
- Information Technology
- Digital Literacy & E-safety

Children will be given an opportunity to:

- become familiar with principles of information and computation, how digital systems work and how to do programming
- create programs, systems and a range of content
- be able to use, express themselves and develop ideas in a digital world

These skills are then applied and developed across all curriculum areas.

An extra curricular club gives children the opportunity to follow their own interests, practise their skills and extend their knowledge.

Teaching and learning strategies

The school interprets Computing as wider than only the weekly Computing sessions using laptops and standalone PCs. Children also have access to programmable toys, equipment in role play areas, digital cameras, iPads, digital video cameras and interactive whiteboards.

During a typical Computing skills lesson the teacher uses the Interactive Whiteboard, laptop or iPad to demonstrate a concept or skills to the whole class/groups then gives time for children to develop their skills. The teacher observes, supports and extends the children as appropriate. (See Learning and Teaching policy)

Assessment and recording

By planning and tracking the use of Computing throughout school, the school will monitor continuity and progression at regular intervals in accordance with the Planning, Assessment and Recording policy.

The school reports progress and attainment to parents at the end of each year.
Computing is used to support assessment, tracking and target setting in other subjects, including English and Maths. The Senior management team uses MIS to track individuals and groups of pupils and identify trends and set targets.

Health and Safety

Health and safety issues specifically using a variety of technology including:

- No one spends long periods working continuously on computers
- The computers are at appropriate heights for the children and the children are shown the correct way to sit
- Care is taken to ensures all leads and cables are stowed safely and securely
- Children are encouraged, when working in pairs or groups at the computers, to make sure everyone can see clearly and is comfortable
- Children are shown how to position their hand on the mouse correctly
- Nothing is placed or stored on top of the monitor’s ventilation grills

- The children are shown how to use mobile equipment such as the digital cameras responsibly
- Electrical appliances are tested regularly by PAT testers
- Fire exits are clearly displayed and all staff are aware of the correct procedures
- Children learn about e-safety. An expert in e-safety visits the school every two years.
- Staff receive e-safety training
- E-safety rules are displayed near PCs.

Equal opportunities

All children regardless of gender, ability, social and cultural background are entitled to be offered a Computing curriculum applicable to their individual needs. The school will ensure this by giving all children equal access to the Computing curriculum and also by using software with different levels of access, specialist hardware and peripherals and additional adult support where necessary. For those children demonstrating greater competency in Computing skills, provision will be made. (See Inclusion Policy and Learning and Teaching Policy).

Staff development

Staff can access training and CPD in computing to develop and enhance their knowledge.
All staff have access to email and the Internet and are encouraged to communicate information in this way.

Resource management

Planning and resources are saved on the school's online system. The ICT teacher has electronic 'How To' guides that other staff can access.

All software licenses are located in a file in the school office. All software is used in strict accordance with the license agreement and no software is copied unless a copyright license to do so is held. No personal software is allowed to be loaded on school computers. Any data files which contain information about living, identifiable individuals is registered under the Data Protection Act.

Role of the ICT Coordinator

The ICT Coordinator role includes:

- Identify and fulfil needs to enable the successful implementation of the Computing curriculum.
- Ensure that suitable Computing planning is in place.
- Monitor and evaluate the implementation of Computing skills ensuring their progression and continuity across the whole curriculum.
- Promote the integration of Computing within the whole curriculum
- Oversee the delivery of the e-safety element of the Computing curriculum.
- Liaise with the e-safety coordinator and governor.
- Encourage and support colleagues where necessary.
- Attend training when necessary.
- Liaise with ICT teacher
- Review the school's Computing policy.
- Keep up to dates with new developments in technology (including hardware and software)

Role of other subject managers

The subject manager's role includes:

- Plan for and monitor the use of Computing within their own subjects, ensuring that the statutory requirements are met.
- Evaluate and select appropriate hardware and software to support learning in their own subjects.
- Identify opportunities for the use of Computing within their area of responsibility.
- Identify opportunities for monitoring and assessment activities within their own area of responsibility.

As a school we will educate and encourage pupils to keep safe.

The content of the curriculum will:

- promote a school ethos which promotes mutual respect and a positive, supportive learning environment
- give pupils a sense of being valued
- promote British Values within a strong Spiritual, Moral, Cultural and Social framework
- prevent radicalisation and/or or the promotion of extremist views
- promote the creation of a culture which helps students to feel safe and able to talk
- encourage pupils to talk freely about their concerns, believing that they will be listened to and valued.

Community links

The school website promotes school and community links. This contains the school prospectus, newsletters and other communications. Children's work is displayed and staff are encouraged to add photographs and examples of work (See E-safety Policy for use of photography and examples of pupils' work). The website is updated regularly.

E-safety and Acceptable Use of IT Policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing and for Child Protection. The school has an e-Safety Coordinator – Sue Boorman. This is also the Designated Safeguarding Lead as the roles overlap. Our e-Safety Policy has been written, building on government guidance. The e-Safety Policy will be reviewed annually.

Application

This policy applies to all stakeholders including the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members. Where elements refer to staff only this will be highlighted.

The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software, school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work.

This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

Access for staff

School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

Official Email

Staff have been provided with a school email address to enable them to perform their role effectively. It would not normally be used to communicate with parents and pupils unless express permission has been provided. Where staff are able to access email outside of school hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

Software Packages

Access to certain software packages and systems (e.g. IBC (HR, finance and procurement system), FFT, school texting services) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

IT Equipment

Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures is followed.

Personal Mobile Phone Use for School Purposes

If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

Mobile Phone Use - Driving

No mobile telephones or similar devices, even those with hands free facilities should be used whilst driving on school business.

School Telephone System

Whether school staff have access to the school telephone system for personal use will be confirmed by the school. Where such use is made of this facility, it must be done during break periods and must not be excessive. The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy for staff who access the computers for a significant period of the working day.

Communication with parents, pupils and governors

The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a member of the senior leadership team where they feel they need to make a telephone call to a parent.

Text System – All Teachers and Office staff. Where other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Leadership team before sending. Where office staff send letters home these will normally require approval by the Office Manager.

Email – school email accounts should not be used for communication with parents unless approved by a member of the senior leadership team. The approved email account is parent.mail@hwis.hants.sch.uk Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the school's policy on home visits.

Communications with Pupils - Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

School Social Media Accounts - The school has official social media accounts that are used to publish material relevant to the school that has been authorised for publication. Only staff authorised to use the official social media accounts are permitted to publish material.

Personal Social Media Accounts – Social media is a part of everyday life and it is normal for staff to have personal social media accounts. It is not acceptable for staff to post any material or comment about the school or its activities on personal social media accounts. School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children (no reference should be made in social media to students / pupils/ parents / carers or school staff). Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal. They should not engage in online discussion on personal matters relating to members of the school community or offer personal opinions which can be attributed to the school or local authority. Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

Unacceptable use of the school IT system
School systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share;
- to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others;
- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material;
- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally;
- to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils;
- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;
- to collect or store personal information about others without direct reference to The Data Protection Act or GDPR provisions.
- to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project;

- to visit or use any online messaging service, social networking site, chat site, web based email or discussion forum not supplied or authorised by the school;
- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people;

For a member of staff, any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Leadership Team.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly. This is managed by our IT contractor and is updated remotely.
- The school uses the HCC Broadband with its firewall and filters.
- Staff log into the school system using their personal login, including a password. Staff are required to keep their passwords secure and confidential.
- Pupils log into the school system using year group logins with no password required.

Internet content

- Pupils will be taught what to do if they see something on the internet that makes them feel uncomfortable or unsafe.
- Where a member of staff accidently or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

- Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited. As staff are not authorised to use official ICT accounts or equipment for personal use there should be no personal data exposed. To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

E-mail

- Pupils will only use approved e-mail accounts on the school system.
- Pupils are to immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The school will promote acceptable behaviour when using an online environment and email, i.e. be polite, do not use any bad or abusive language or other inappropriate behaviour;
- Use of words included in the Policy Central 'banned' list will be detected and logged.
- Whole-class or group e-mail addresses will be used when necessary.
- Pupils must not download any files (including any attachment in e-mails), without permission.

Published content and the school website

- The point of contact on the website will be the school address, telephone number and a general email contact address, e.g. parent.mail@hwis.hants.sch.uk .
- Home information or individual e-mail identities will not be published.
- The content of the website will comply with the statutory DfE guidelines for publications.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate and the quality of presentation is maintained.
- Most material will be the school's own work; where other's work is published or linked to, the school will credit the sources used and state clearly the author's identity or status.
- Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.
- Embedded geodata will not to be used in respect of stored images
- Pupils will have access to software that is password protected and run from the school website (e.g. Purple Mash, Education City).

Overview of the e-safety requirements for school.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs and examples of work.
- Pupils' names will not to be used when saving images in the file names or in the tags when publishing to the school website;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

- Social networking sites and 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 or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

Use of personal devices

- No personal IT equipment is to be connected to school IT systems.
- Staff must not store or export any images of pupils or pupil personal data on, or to, any personal devices.

CCTV

- CCTV is in use in the school as part of our site surveillance for staff and student safety. Any recordings will not to be revealed without permission except where disclosed to the Police as part of a criminal investigation.
- Specialist video recording equipment used as part of classroom activities will not be revealed on any occasions outside of the staff and will not be used for any other purposes.

Managing filtering

- The school will work in partnership with the HCC to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.

General use of mobile phones

- Mobile phones and personally-owned devices may not be used during lessons or formal school time. They should be switched off (or on silent).
- Mobile phones and personally-owned mobile devices brought in to 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.
- Personal mobile devices will not be used during lessons.

Staff use of personal devices - Personal and private use

- All school staff with access to computer equipment, including email and internet, are **not** permitted to use them for personal use.
- Personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.
- It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.
- Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops or cameras into the school, these personal items should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff

should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

- Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 3.
- Staff are not permitted to use their own mobile phones or devices for contacting pupils, young people or those connected with the family of the student.
- 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.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to break times, lunchtime and after school.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Mobile phones should be switched off (or turned onto 'silent' mode) and left in a safe place during lesson times.

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. School mobiles are available for trips. Staff are permitted to take their own mobiles with them on trips in case of personal emergency but they are not to be used routinely. Parent helpers and others (e.g. students and volunteers) are required to sign a volunteer helpers' agreement covering the use of mobile devices and will be reminded about school policy on phones and cameras when on trips.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations (See Data Protection Policy for full guidance)

Passwords

Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.

Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the acceptable Computing Use Agreement, 'E-Safety Agreement Form for School Staff', before using any school Computing resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Assessing risk

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 HCC can accept liability for the material accessed, or any consequences of Internet access.
- Pupils will be taught rules for the responsible use of computers, Internet and related technologies.
- Pupils will be taught where to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organization such as Childline (0800 1111) or the CLICK CEOP button (dolphin icon on each laptop and standalone PC in the school) http://ceop.police.uk/safety-centre/
- School will ensure that staff and pupils are aware of regulations regarding copying materials from the web. Staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

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 safeguarding/child protection procedures.

Communications Policy
Introducing the e-safety policy to pupils

- Children will be taught about e-safety and how to keep themselves safe when using the Internet.
- Pupils will be informed that Internet use will be monitored.
- An e-Safety education programme will be introduced and kept running to raise the awareness and importance of safe and responsible internet use.
- E-safety will be embedded into ICT lessons.
- An e-safety expert will visit school every two years to work with all children (and parents, where possible) to further develop their understanding of e-safety.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

School will run advice, guidance and training for parents which will include:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safety behaviour are made clear.
- Information leaflets in school newsletters and on the school website.
- Suggestions for safe Internet use outside school i.e. home.
- Provision of information about national support sites for parents.

Security and confidentiality

- Any concerns about the security of the ICT system should be raised with a member of the leadership team.
- Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.
- School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with an encrypted data device for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's leadership team.
- Where staff are permitted to work on material at home and bring it in to upload to the school server through encrypted data devices, they must ensure that they have undertaken appropriate virus checking on their systems. Where provided, staff should normally use their school issued laptop for such work.
- The school has nominated Inspired IT to be responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify InspiredIT when reporting any concerns regarding potential viruses, inappropriate software or licences.
- Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, with an encrypted data device. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.
- Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

Whistleblowing and cyberbullying

- Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephones, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL). Complaints of a child protection nature must be dealt with in accordance with school safeguarding/child protection procedures.
- It is recognised that increased use of ICT can led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.
- Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in Cyber bullying: Practical Advice for School Staff.

- School will teach pupils about the impact of cyberbullying and pupils will know how to seek help if they are affected by any form of online bullying (including in e-mails and related technologies).

Appendix 1

For Staff of Hatch Warren Infant School – E-safety agreement

- I appreciate that ICT includes a wide range of systems, including mobile phones, cameras, email, internet, HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted.
- I understand that I must not communicate information which is confidential to the school or which I do not have the authority to share.
- I understand that school information systems and hardware may not be used for personal or private use without the permission of the Headteacher.
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance.
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication.
- I understand that I must not use the school ICT system to access inappropriate content.
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will follow the school's policy in respect of downloading and uploading of information and material.
- I will ensure that school data / information is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep school data / information on removable storage devices. Where it is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights.
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher in accordance with school safeguarding/child protection procedures.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors.
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted.

- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites.
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and where activities undertaken are inconsistent with expectations of staff working with children.
- I will ensure that all information relating to school is accessed via the School Dashboard or saved to an encrypted data stick/hard drive which restricts access to only authorised personnel.

Staff Commitment
The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.
I have read and understand the Computing and E-safety Policy and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Leadership Team.

Signed: ………………………………………………………….. Name: ……………………………………………………………

Accepted for School:

SBoorman

Name: Sue Boorman, Headteacher

Date: …………………………………..

This form is valid for the time the staff member is employed at the school and will automatically expire after this time.

Appendix 2

Do's and Don'ts: Advice for Staff
Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately, if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do:

- ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources
- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- be aware that the school's systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- seek approval before taking personal data off of the school site
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead as appropriate
- be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in ICT
- ensure that your use of ICT bears due regard to your personal health and safety and that of others

Don't

- access or use any systems, resources or equipment without being sure that you have permission to do so
- access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
- compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
- use systems, resources or equipment for personal use.
- use other people's log on and password details to access school systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use school systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of email, the internet, VLEs and school and HCC intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't

- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet
- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required
- use school mobile telephones when on educational visits

Don't

- send messages that could be misinterpreted or misunderstood
- use the school's telephone system for personal calls (unless authorised to do so)
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pictures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
- put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Appendix 3

For Parents of Hatch Warren Infant School – E-safety agreement

Parent / guardian/carer name: ___________________________________

Pupil name(s): ___________________________________

Parent's Consent for Web Publication of Work and Photographs
I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rules.

Parent's Consent for Internet Access
I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered and monitored service, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent / guardian signature: ________________________________

Date: ___/___/___

This form is valid for the period of the time your child attends this school and will automatically expire after this time.

Appendix 4

Keeping Safe:

stop, think, before you **Click!**

12 rules for the responsible use of computers, internet and related technologies

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for schoolwork and homework.
2. I will only delete my own files.
3. I will not look at other people's files without their permission.
4. I will keep my login and password secret.
5. I will not bring files into school without permission.
6. I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
7. I will only e-mail with the explicit permission of a teacher/teaching assistant/special needs assistance.
8. The messages I send, or information I upload, will always be polite and sensible. The forwarding of chain letters is not permitted.
9. I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
10. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
11. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
12. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix 5

E safety incident log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*
	When:	**When:**
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		
Signature (Headteacher)	**Date**	
Signature (Governor)	**Date**	