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January 2023	Major	JF	Amendments to out-of-date information
September 2025	Major	JF	Completely new Computing policy due to change of scheme we are now using. E-safety and Acceptable Use of IT Policy similar to previous version. Some of the 'dos and don'ts' pages removed from Appendices

About This Document

This policy sets out Hatch Warren Infant School's aims and strategies for the successful delivery of Computing. This policy should be read in conjunction with other relevant school policies such as the Safeguarding, Prevent, Equal Opportunities, Curriculum, Finance, Teaching & Learning, SEND and Assessment policies.

Aims

The school aims to develop independent learners who are well equipped for their future. Hatch Warren Infant School believes that every child should have the right to a curriculum that champions excellence and enables pupils to achieve to the very best of their abilities. We understand the immense value technology plays not only in supporting the Computing and whole school curriculum but overall in the day-to-day life of our school. We believe that technology can provide enhanced collaborative learning opportunities, better engagement of pupils and easier access to rich content. It can also support conceptual understanding of new concepts and support the needs of all our pupils.

Our Aims:

- Provide an exciting, rich, relevant and challenging Computing curriculum for all pupils.
- Teach pupils to become responsible, respectful and competent users of data, information and communication technology.
- Enthuse and equip children with the capability to use technology throughout their lives.
- Give children access to a variety of high quality hardware, software and unplugged resources.
- Equip pupils with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise risk to themselves and others.
- Instil critical thinking, reflective learning and a 'can do' attitude for all our pupils, particularly when engaging with technology and its associated resources.
- Use technology imaginatively and creatively to inspire and engage all pupils, as well as using it to be more efficient in the tasks associated with running an effective school.

Safeguarding: Online Safety

Online safety has a high profile for all stakeholders at Hatch Warren Infant School. We ensure this profile is maintained and that pupil needs are met by the following:

- A relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 2
- Our home/school links and communication channels ensure that parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.
- Data policies stipulate how we keep confidential information secure.
- Online safety is threaded throughout other curriculums and embedded in the day-to-day lives of our pupils.
- Training for staff and governors is relevant to their needs and positively impacts on the pupils.
- Our online safety policy (part of our safeguarding policy) clearly states how monitoring of online safety is undertaken and any incidents/infringements to it are dealt with.
- Filtering and monitoring systems are in place for all our online access.

Curriculum

As a school, we have chosen the Purple Mash Computing Scheme of Work from Reception to Year 2. The scheme of work supports our teachers in delivering fun and engaging lessons which help to raise standards and allow all pupils to achieve to their full potential. We are confident that the scheme of work meets the national vision for Computing. It provides immense flexibility and strong cross-curricular links. Furthermore, it gives excellent supporting material for less confident teachers.

Early Years

We aim to provide our pupils with a broad, play-based experience of Computing in a range of contexts. We believe the following:

- Early Years learning environments should feature ICT scenarios based on experience in the real world, such as in role play.
- Pupils gain confidence, control and language skills through opportunities such as 'painting' on the interactive board/iPads and controlling Bee-bots and remotely operated toys.
- Outdoor exploration is an important aspect of Early Years and experiences should be enhanced by ICT toys such as metal detectors, controllable toys and telephone sets.
- Recording devices can support children to develop their communication skills.

Key Stage One Outcomes

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Organise, store, manipulate and retrieve data in a range of digital formats.
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school

Assessment

Pupil attainment is assessed using attainment statements and detailed exemplification that is provided for each key learning intention. Work from all classes and a range of abilities is monitored by the Computing Manager. Teachers keep accurate records of pupil attainment by entering data onto the school tracking document. Tracking of attainment is used to inform future planning. Children are encouraged to self, peer and group assess work in a positive way. Formative assessment is undertaken each session in Computing and teachers use the

progression of skills document to evaluate progress. Summative assessment is undertaken in line with the assessment cycle (See Assessment Policy).

Inclusion

At Hatch Warren Infant School, we aim to enable all children to achieve to their full potential. This includes children of all abilities, social and cultural backgrounds, those with SEND and EAL speakers. We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEN and disabilities. With this in mind, we will ensure additional access to technology is provided throughout the school day for children who require it.

Monitoring, Evaluation and Feedback

Monitoring will be achieved through:

- work scrutiny
- learning walks
- observations
- pupil voice
- teacher voice
- reflective teacher feedback

Evaluation and Feedback will be achieved through:

- Dedicated Computing Leader time
- Using recognised standards documentation for end-of-year expectations
- Written feedback on evaluation of monitoring activities to be provided by the Computing Leader in a timely manner
- Feedback on whole school areas of development in regard to Computing to be fed back through INSET/AOB/staff meetings

Roles and Responsibilities

Due to technology extending beyond the National Curriculum for Computing, there are key roles and responsibilities specific members of staff have.

Head Teacher

- Monitoring the implementation of the Computing Policy and its associated policies such as the Safeguarding and SEND Policies.
- Ratifying (in conjunction with the Governing Body) the Computing policy, Safeguarding policy and Computing Leader's Action Plan
- Securing technical support service contracts and infrastructure maintenance contracts.
- Approving CPD and training which is in line with the whole school's strategic plan.
- Setting and approving budget bids
- Creating in conjunction with the Computing Leader, a long-term vision for Computing which includes forecasted expenditure and resources
- Monitoring the performance of the Computing Leader in respect to their specific job role description for Computing
- Ensuring any government legislation is being met

Computing Subject Leader

- Raising the profile of Computing

- Monitoring the standards of Computing and feeding back to staff in a timely fashion so they can act on areas for development
- Ensuring assessment systems are in place for Computing
- Maintaining overall consistency in standards of Computing across the school
- Reporting on Computing at specific times of the year to the Governing Body/Head/Staff
- Auditing the needs of the staff in terms of training/CPD
- Supporting staff with their day-to-day practice and sharing new ideas, approaches and initiatives
- Attending training and keeping abreast with the latest educational technology initiatives
- Using nationally recognised standards to benchmark Computing
- Creating Action Plans for Computing
- Reviewing the Computing curriculum and developing it as needed
- Working as needed with the Head Teacher to ensure online safety provision is above adequate and all legislation is in place

Technician

- Conducts routine scheduled maintenance/updates on systems
- Supports the administration and set-up of online services including the school website
- Fixes errors/issues with hardware and software
- Routinely checks school filtering, monitoring and virus protection
- Maintains network connectivity and stability
- Sets up new hardware and installations
- Supports the Head Teacher with future infrastructure needs and associated projected costs

Administration Staff

- Maintains the school website content
- Posts approved requests to the school's social media accounts
- Supports procurement of resources and technical services
- Supports the technician with some data management

Health and Safety

Hatch Warren Infant School takes all necessary measures to ensure both staff and pupils are aware of the importance of health and safety. Both staff and pupils are trained to handle electrical equipment correctly including how to power on and off.

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 – Headteacher. 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 In Arbor App messages 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 is 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.

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.

Display Screen Equipment
The school will ensure that 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.

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.

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.

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 .
- 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).

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.

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)

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.
- E-safety will be embedded into Computing lessons and other areas of the curriculum (e.g. PSHE).

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 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 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.

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:

Name: Sue Boorman, Headteacher

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:	**Don't:**
• 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	• access or use any systems, resources or equipment without being sure that you have permission to do so
• ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources	• 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
• ensure that where a password is required for access to a system, that it is not inappropriately disclosed	• compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
• respect copyright and intellectual property rights	• use systems, resources or equipment for personal use.
• be aware that the school's systems will be monitored and recorded to ensure policy compliance	• download, upload or install any hardware or software without approval
• ensure you comply with the requirements of the Data Protection Act when using personal data	• use unsecure removable storage devices to store personal data
• seek approval before taking personal data off of the school site	• use school systems for personal financial gain, gambling, political activity or advertising
• ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely	• communicate with parents and pupils outside normal working hours unless absolutely necessary
• 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	
• 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	

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

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**	