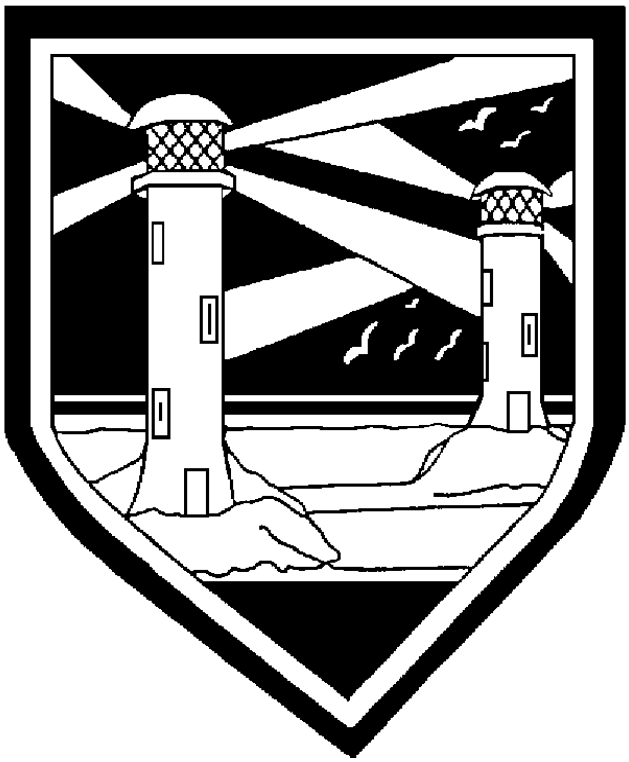
Harwich Community Primary School and Nursery



E-safety Policy

E-safety Responsibility: Mrs R Anderson
E-safety Governor: MR Adrian Mann

Document approved by staff:	Sept 2024
Document approved by governors:	Sept 2024
This Document is due for review:	Sept 2025

CONTENTS

1. INTRODUCTION

ICT and computing in the 21st Century are an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children. Harwich Community Primary School and Nursery recognises the need to build in the use of these technologies in order to educate our pupils.

Information and Communication Technology and Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Email, Social Media, Instant Messaging and chat rooms ;
- Mobile/ Smart phones with text, video and/ or web functionality;
- Other mobile devices with web functionality;
- Gaming, especially online;
- Learning Platforms and Virtual Learning Environments.

Schools have a duty of care to support parents in understanding the issues and risks associated with children's use of digital technologies. Harwich Community Primary School and Nursery takes an active role in providing information and guidance for parents on promoting E-safety messages in home use of ICT.

Whilst exciting and beneficial, both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (e.g. 13 years for Facebook).

At Harwich Community Primary School and Nursery we understand the responsibility to educate our pupils on E-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies.

2. WRITING AND REVIEWING THE E -SAFETY POLICY

The E-safety Policy relates to the School's safeguarding policies and practices, as well as to other policies including those for ICT, Anti-Bullying and Child Protection. Our E-safety Policy has been written by the School, building on Government guidance and recommendations. It has been agreed by all staff and approved by Governors. The E-safety Policy and its implementation will be reviewed annually.

3. SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, and community users) who have access to and are users of school computing systems, both in and out of school.

4. 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 will provide pupils 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;
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.

Internet use will Enhance Learning

- The School's Internet access will be designed for pupil use and will include filtering appropriate to the age of pupils;
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- Pupils will be educated in the effective and safe use of the Internet in research.

Pupils will be Taught how to Evaluate Internet Content

- The School will ensure that the use of Internet derived materials by staff and pupils complies with copyright law;
- Pupils should be taught to be aware of the materials they read and shown how to validate information before accepting its accuracy;
- Pupils use the Internet widely outside school and will learn how to evaluate Internet information and to take care of their own safety and security.
- E- Safety will feature regularly within the Computing lessons.

5. ROLES AND RESPONSIBILITIES

Governors:

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-safety incidents and monitoring reports. A member of the Governing

Body has taken on the role of E-safety Governor. The role of the E-safety Governor will include:

- Regular meetings with the E-safety Co-ordinator Mrs R Anderson;
- Regular monitoring of E-safety incident logs;
- Regular monitoring of filtering;
- Reporting to relevant Governors at committee meetings.

Training – Governors

Governors should take part in E-safety training and awareness sessions, with particular importance for those who are members of any sub-committee or group involved in Computing, E-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation;
- Participation in school training and information sessions for staff or parents.

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including E-safety) of members of the school community and is also responsible for ensuring that the relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the E-safety Co-ordinator.

The Headteacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff (see Whistleblowing Policy).

The E-safety Coordinator:

- Takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies and documents;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place;

- Provides training and advice for all staff;
- Liaises with the Local Authority;
- Receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments;
- Meets regularly with E-safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- Attends relevant Governors meetings;
- Reports regularly to the Governors and Senior Leadership Team.

ICT Technician:

The ICT Technician is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack;
- That the school meets the E-safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority E-safety Policy and guidance;
- That users may only access the school's networks through user names;
- The LA is informed of issues relating to the filtering applied;
- The school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- They keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant;
- That the use of the network and email are regularly monitored in order that any misuse or attempted misuse can be reported to the E-safety Co-ordinator, Headteacher or Senior Leader for investigation and if necessary, action and sanction;
- That monitoring software systems is implemented and updated as agreed in school policies.

Teaching and Support Staff:

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

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and of the current school E-safety policy and practices;
- They report any suspected misuse or problem to the E-safety Co-ordinator, Headteacher or Senior Leader for investigation, and if necessary, action and sanction;
- Digital communications with pupils and/or parents should be on a professional level and only carried out using official school systems.

- E-safety issues are embedded in all aspects of the curriculum and other school activities such as assemblies;
- Pupils understand and follow the school E-safety rules;
- Are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found through Internet searches;
- Staff must not give personal contact details to pupils or parents/carers including details of any blogs, social network accounts or personal websites;
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted;
- If a member of staff uses a social network site, details must not be shared with pupils and privacy settings be set at maximum.

Training – Staff

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal E-safety training will be made available to staff as part of the termly CPD programme;
- All new staff will receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Policy;
- The E-safety Coordinator will receive regular updates through attendance to meetings and training events, Local Authority courses and any other information or training sessions deemed appropriate or necessary. They will also review updated guidance and documents released;
- This E-safety Policy and its updates will be presented to and discussed by staff in staff meetings;
- The E-safety Coordinator (or other nominated person) will provide advice, guidance and training to individuals as required;
- Staff should act as good role models in their use of ICT, the Internet and mobile devices;

Introducing the E-safety Policy to Pupils

E-safety rules will be posted in all class rooms and the ICT suite and discussed with the pupils at the start of each year and at the beginning of each unit of work. Pupils will be informed that network and Internet use will be monitored. The school will hold termly assemblies with an E-safety theme.
Pupils are also responsible for ensuring that:-

- They use the school ICT systems in accordance with the Acceptable Use Policy, (which parents/carers sign on behalf of the pupils before being given access to school systems) and the E-safety Charter created by pupils on a yearly basis;
- Need to understand the importance of reporting inappropriate materials and know how to do so;
- Will be expected to know and understand how to keep safe online and when using mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and using images and on cyber-bullying;
- Should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school.

Education – pupils

E-safety education will be provided in the following ways:

- In accordance with the 2014 National Curriculum requirements, planned E-safety teaching will be provided as part of Computing/PSHE/other curriculum areas (as relevant) and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school;
- Key E-safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities;
- KS2 pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information;
- Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Rules for use of school computers, laptops, I Pads and the Internet will be revised annually through discussion with pupils. These will be posted in classrooms and displayed on the E-safety display board.

Parents/Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the Internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Therefore parents and carers are responsible for:

- Being vigilant and taking an active role in monitoring and regulating their children's online experiences.

Education – Parents/Carers

Parents and Carers undoubtedly play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences.

With this in mind, the school will seek to take every opportunity to help parents and carers and provide information and awareness on safety issues through:

- Parents' meetings;
- Letters and newsletters;
- The school website;
- Ensuring information about national and local E-safety campaigns and literature is disseminated;
- Drawing parents' attention will be drawn to the School E-safety Policy in newsletters and on the website;
- Ensuring our website now has an E-safety section for parents with information leaflets on web safety, cyberbullying and other important information that is relevant and this is regularly updated.

Harwich Community Primary School and Nursery believes that working in partnership with parents and carers will enhance the E-safety of our pupils and help them develop a healthy relationship with the internet.

6. COMMUNICATION TECHNOLOGIES

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored;
- Users need to be aware that email communications may be monitored;
- Users must immediately report, to the Headteacher – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

The school uses a variety of communication technologies and is aware of the benefits and associated risks:

Pupil Email

- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
- Pupils use a virtual email software to teach this;
- Pupils must immediately tell a teacher if they receive an offensive email;

- Pupils must not reveal personal details of themselves or others in email communications, or arrange to meet anyone without specific permission;
- The forwarding of chain emails is not permitted.

Staff Email

- Only official email addresses are to be used between staff and with pupils/parents and must be professional in nature, tone and content;
- The email has a filtering service that reduces the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be reported to the IT technician;
- All staff are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school;
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

Social Networking and Personal Publishing

Social network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Instagram and Twitter. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a social network site, you may have access to view other users' content, send messages and leave comments.

- The School blocks/filters access to all social networking sites;
- 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 attended, email address, full names of friends, specific interests and clubs, etc;
- Pupils and parents will be advised that the use of social network sites outside school have age restrictions for pupils' own protection (e.g. Facebook – 13 years). **Therefore no children of primary school age should have their own social media accounts.**

Mobile Telephone

- The School allows personal mobile phones to be used in school by staff and visitors but they are asked to be left on silent in curriculum time and are not used during lessons/duty;
- It is acceptable to use personal mobile phones for school activities e.g. school trips;
- Personal mobile phones should be locked with a passcode /swipe code;
- Pupils who bring mobile phones into school do so at their own risk. They must hand them into the office at the start of the school day and pick them up again at the end of school.

iPads/Tablets

- Any personal or school owned laptops, IPads or tablets must be locked with a passcode/swipe code.
- No photographs of pupils should be taken on personal phones or devices and should only use the school cameras / I pads.

Websites and other Online Publications

This may include for example, podcasts, videos and blogs.

- The School website is effective in communicating E-safety messages to parents/carers;
- Everybody in the School is made aware of the guidance for the use of digital media on the website;
- Staff responsible for editing the website are aware of the guidance regarding personal information and safeguarding;
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified;
- Pupils' work and photographs will only be published if consent has been given by the parents/carers;
- The Headteacher has overall responsibility for what appears on the website.

7. MANAGING INTERNET ACCESS

Information System Security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. 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 on-line activities that will support the learning outcomes planned for the pupils' age and maturity. The school will work with the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the E-safety Co-ordinator. Senior staff will see that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Technical – infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school ICT systems;
- All users will be provided with a username and password by the ICT technician who will keep an up to date record of users and their usernames;
- The "administrator" passwords for the school ICT system, used by the ICT Technician must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe);
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be carried out by a process that is agreed by the Headteacher (or other nominated senior leader);
- Any filtering issues should be reported immediately to the E-safety Co-ordinator;
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician and Mrs Anderson;
- The school ICT Technician and the Headteacher regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. An appropriate system is in place for users to report any actual or potential E-safety incident;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. students, visitors) onto the school system;
- An agreed policy is in place that restricts staff from installing programmes on school workstations and / or portable devices;
- Shared expectations around the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations / portable devices is a regular agenda item at staff meetings.

Curriculum

E-safety is a continuing focus in all areas of the curriculum and staff reinforce E-safety messages, wherever possible, in the use of Computing across the curriculum. We also have a safety dolphin icon that the children are fully aware of.

- Processes are in place for dealing with any unsuitable material that is found during Internet searches (This is dealt with by ECC);

- Where pupils are allowed to freely search the Internet, eg using search engines, staff will be vigilant in monitoring the content of the websites the young people visit, thus encouraging responsible use.

Use of digital and video images

When using images and video, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the Internet. It is vital both staff and pupils are aware of and take responsibility for their digital footprint. Images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, using and sharing images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites;
- Staff are allowed to take digital and video images to support educational aims, but will follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, under no circumstances should the personal equipment of staff be used for such purposes;
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the school's Home School Agreement (which seeks parental consent) on the use of images;
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or the school's social network accounts. An updated list will be kept by the E Safety Co-ordinator, the Headteacher and the school office. This list will also available to all staff.

Data protection

We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998. Staff will ensure they properly log-off from a computer terminal after accessing personal data and will not remove personal or sensitive data from the school premises without permission of the Headteacher. Any data which is impractical to ensure is kept in school (e.g. Reports) will be kept secure, by use of encrypted memory sticks which are password protected.

8. HANDLING E-SAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team;
- Any complaint about staff misuse must be referred to the Headteacher. A complaint about the Headteacher should be referred to the Chair of Governors;
- Complaints of a Child Protection nature must be dealt with in accordance with the School's Child Protection procedures;
- Pupils and parents will be informed of the complaints procedure.

APPENDIX 1 - ACCEPTABLE USE POLICY

Use of the Internet is now an integral part of people's lives. In spite of this, it is important schools continue to be aware of issues and problems and to continue to educate our children accordingly. It is important staff, pupils and parents understand the moral and ethical issues surrounding access to the Internet before allowing access.

There are a number of options available that restrict access to the Internet, but it must be understood that no system, other than a ban on using the Internet, can ensure users do not access material that is deemed inappropriate. Pornographic material is usually the main focus of filtering methods, but users need to be aware that removing racist, sexist and political material is beyond many filtering programs. There is also the difficulty with any filtering software that content which is deemed offensive to one group of people is regarded differently by others. Furthermore, we are now faced with more recent issues such as grooming, cyber-bullying, extremism and identity theft which cannot always be controlled by filtering systems. For these reasons, treating the use of the Internet as an issue that involves pupils, staff and parents has to be the most sensible approach.

In response to this, the most appropriate course of action is to develop a school policy on use of the Internet together with a home/school agreement.

Harwich and Community Primary School and Nursery has this Acceptable Use Policy, together with rules for safe internet use. These rules are a joint agreement between staff and pupils as part of our E-safety Curriculum. The policy works in line with our Home School Agreement and is available to parents on request and electronically via our website.

Today millions of people use the Internet and e-mail on a daily basis. In recent years, use of the Internet has continued to increase, particularly with the introduction of mobile devices. This is not only for business and personal use, but also for educational purposes. A wealth of educational resources are now available on the Internet and via mobile devices; and this continues to grow. At Harwich Community Primary School and Nursery, we believe that our pupils should have opportunity to use these emerging and changing technologies to support their learning and to equip themselves with the skills that will be required for lifelong learning.

Resources found on the Internet, are unlike those found in more traditional media. Historically, resources such as books, videos and other resources could be carefully selected for the learning process. The Internet, by its open and dynamic nature, may lead pupils to find material over which the teacher has had no previous viewing and has therefore been unable to judge its suitability for classroom use. Although the school will endeavour to point pupils to relevant curriculum sites or to previously researched sites that have been

identified as being relevant to the area of study, we also accept our responsibility in educating our pupils about responsible, respectful and safe use of the Internet.
Research using electronic methods is now fundamental to preparing pupils for citizenship and future possibilities. The school will ensure that opportunities for both integrating the use of the Internet into the curriculum and teaching pupils about E-safety will be planned and that staff will guide pupils in line with Government guidelines.

The school recognises that training the staff in preparation for using the Internet and indeed any mobile technology in a safe manner is vital. The school will use a variety of agencies to train the staff in integrating new technologies into the curriculum. Staff will be given regular opportunities to discuss issues surrounding the use of the Internet and e-safety and develop appropriate teaching strategies. In addition, relevant Governmental guidelines will be made available to all staff as a point of reference.

The school uses an Internet Service Provider (ISP) that has filtering software in place to minimise the risk of accessing inappropriate Internet material or receiving inappropriate e-mail. Should any pupils access material they have concerns about, they should notify a member of staff, who will then inform the E-safety Co-ordinator. The E-safety Co-ordinator will then ask the ICT Technician to inform the ISP of the address of the offending web site. Where possible, appropriate action will then be taken to block further access. On occasions where a total block is not possible, staff will then use this to remind pupils of their own responsibilities in becoming safe users, in line with the Computing curriculum. The school will take appropriate action against users that use the school facilities to knowingly access, or attempt to access inappropriate materials. Therefore, the school reserves the right to access the work area of any user to view files held in that area.

All pupils across the school have access to the Internet and are able to use the technology available. It is anticipated that access to younger pupils will be more directed, with autonomous use being available to older pupils. Where pupils are given freedom to search the Internet for information, they will be given clear learning objectives by their teacher. In the event of inappropriate use or the accessing of inappropriate materials, action will be taken by the teacher, E safety Co-ordinator or the Headteacher. Any incidents will be reported and logged by the E safety Co-ordinator.

Pupils will be taught to use e-mail, the Internet and mobile technology responsibly to reduce the risk to themselves and others. After being agreed by staff and pupils at the beginning of each year, rules for Internet access and the use of all technologies within school will be posted in each classroom and around the school. E-safety will form an integral part of Computing lessons but will also be covered in regular assemblies and as part of our PSHE programme of study.

The school believes that access to the Internet and mobile devices will enable pupils to explore resources available from libraries, other schools, Local Authority and commercial

content providers in a way that will enhance the learning process in ways impossible by other means. E-mail will allow communication to be made with other individuals and organisations, regardless of time and distance.

Older children will be encouraged to accept some responsibility for their use of the Internet and will be asked to sign a pupil E-safety declaration.

The final responsibility for use of the Internet and E-safety lies with the parents and guardians of our pupils. Therefore, the school asks parents to sign our Home School Agreement and our regular E-safety updates. In doing so, parents are giving their permission for their children to be educated in accordance with school policies. Parents will also be provided with support and guidance in maintain their children's safety away from school, through regular events in school and through documentation provided on our website. Such information will also be available in hard copies from the school, should this be required.

This policy will be reviewed on a regular basis in line with the E-safety Policy and any technological advances and developments.

The school will adapt and update the E-safety Policy in light of emerging new technologies and any issues or risks associated with these technologies.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Parents and pupils will be asked to sign and return an 'ICT Acceptable Use Agreement' at the start of each key stage and during an admission interview for pupils who start mid-year.

Acceptable Use Policy for EYFS and KS1 pupils at Harwich Community Primary School and Nursery.

- I will only use what I have been told to.
- I won't upset people on purpose using ICT.
- I will tell an adult if I see something that upsets me.
- I know not to tell people on the internet my personal information.
- I know that I will be in trouble for not following these rules.

Pupil name..... Signed.....

Acceptable Use Policy for children in KS1

Think before you click

S	**Surfing: I will only use the Internet and e-mail with a teacher.**
A	**Access: I will only use the computers if a teacher has asked me to.**
F	**Friendly: I will only send friendly and polite e-mail messages.**
E	**Eeek!: If I see something I don't like on a computer, I will always tell an adult.**

My name:	
My signature:	
Parent/Carer name: (or Parent/Carer signature)	

Acceptable Use Policy for KS2 pupils at Harwich Community Primary School and Nursery pupils

- I always ask permission from an adult before using the internet;
- I only use websites and search engines that my teacher has chosen;
- I use my school computers for school work unless I have permission otherwise;
- If I bring my own personal devices/mobile phone to school, I will hand it in during morning registration. It will be kept in the school office and returned to me at the end of the day. In an emergency, I will ask my teacher before using my own personal devices/mobile phone and do so with an adult present;
- I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult;
- I always credit the person or source that created any work, image or text I use;
- I only talk with and open messages from people I know and I only click on links if I know they are safe;
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened;
- I only send messages which are polite and friendly;
- I keep my personal information safe and private online;
- I will keep my passwords safe and not share them with anyone;
- I will not access or change other people's files or information;
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission;
- I understand that the school's Internet filter is there to protect me, and I will not try to bypass it;
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult;
- I know that my use of school computers and Internet access will be monitored;
- I will only use tablets at school when an adult is present to supervise;
- I will not save anything on the 'Pupil Shared' area of the school network that is unrelated to learning;
- I know that if I do not follow the rules then there will be consequences, depending on the seriousness of my actions, which may include:

  - Missing a playtime;
  - Missing a lunch time;
  - A meeting with my parent and a senior member of staff or the E-safety Co-ordinator.;

- Loss of privileges (such as loss of access to the school computer system, exclusion from a disco etc.);
- Fixed term exclusion.

- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page or turn off the screen and tell an adult straight away, who will help me;
- I have read and talked about these rules with my parents/carers;
- If I am aware of anyone being unsafe with technology then I will report it to a teacher;
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online;
- I know that anything I share online may be monitored;
- I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend;
- I am aware of the CEOP (Child Exploitation and Online Protection) report button and know how and when to use it.

Pupil Full Name:

Pupil Signature:

Date:

Acceptable Use Policy for adults and staff at the Harwich Community Primary School and Nursery.

This policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- Only use, move and share personal data securely and ensure that removable data storage devices are encrypted or are password protected;
- Respect the school network security;
- Implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources;
- Respect the copyright and intellectual property rights of others;
- Only use approved email accounts;
- Only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site;
- Only give permission to pupils to communicate online with trusted users;
- Use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues;
- Not use or share my personal (home) accounts/data (e.g. Facebook, Twitter, Instagram, email, eBay etc.) with pupils;
- Set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs);
- Report unsuitable content and/or IT misuse to the named E-safety Co-ordinator;
- Promote any supplied E-safety guidance appropriately;
- Return school IT equipment to the school without delay at the request of the ICT Technician or School Senior Leadership Team.

I know that anything I share online may be monitored. I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

Visit internet sites and make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to;

- Pornography (including child pornography);
- Promoting discrimination of any kind;
- Promoting violence or bullying;
- Promoting racial or religious hatred;

- Promoting illegal acts;
- Breach any Local Authority/School policies;
- Enter into any communication that may bring The Harwich and Community Primary School and Nursery, or its staff, pupils or any other stakeholder into disrepute;
- Do anything which exposes others to danger;
- Access any other information which may be offensive to others;
- Forward chain letters;
- Breach copyright law;
- Use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission;
- Store images or other files off site without permission from the Headteacher or their delegated representative;

I will ensure that any private social networking sites, blogs, etc. that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Staff Full Name:

Staff Signature:

Date:

APPENDIX 2 – LETTER TO PARENTS

Dear Parents,

Re : Responsible Use of the Internet

I ask that you read this letter and the attached policy and then sign and return the slip to school.

Millions of people today use the Internet and e-mail as part of their daily lives. At Harwich Community Primary School and Nursery, we recognise this, and believe our pupils should have the opportunity to learn about and use these emerging and changing technologies. This will not only help to support their learning across the curriculum but also equip the children with the skills they will require for life-long learning.

In order to develop their learning, our children have regular access to computers, laptops, mobile devices and to the Internet throughout the school. We are fully aware of the concerns and issues surrounding safe Internet use and have a clear policy in place for dealing with this, a copy of which is attached to this letter. Our Internet provider is filtered and any computer use is monitored by staff. E-safety rules are agreed by staff and pupils at the start of each year. These are displayed throughout the school and are available to view on our website. Children in KS2 also have a safe computer use contract which they are asked to sign.

Should you have any further concerns or wish to discuss any aspect of Internet use, please do not hesitate to contact me at the school.

Yours sincerely,

Mrs Anderson

Head Teacher / E-safety Co-ordinator

PLEASE COMPLETE AND RETURN THE FOLLOWING SECTION

I have read and accept the Acceptable Use Policy for pupils.
I give my permission for my son/daughter to use the Internet as part of their learning at Harwich Community Primary School and Nursery.
I understand that suitable guidance and supervision will be provided during access to the Internet.
Signed_____ PRINTED: _____Date _____
Name of son/daughter _____ Class _____