E – Safety

The Acceptable use of the Internet and Related Technologies

Reviewed Autumn 2016

Contents

Appendicies

Our E-safety policy

The E-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

The school's E-Safety Coordinator is the head teacher; Mrs Emily Morris.
Mrs Morris is also the school's Child Protection Co-ordinator.

It has been agreed by senior management and approved by governors.

The E-Safety Policy was revised, Autumn 2017

Introduction to E-Safety

1.1 E-Safety in a Changing World

The term E-safety covers the issues relating to young people and staff and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

At Eastway Primary School we celebrate the value and importance of technology in our children's learning. In our school; personal computers, wireless laptops, digital voice recorders, camcorders and digital cameras are all part of children's every day learning. The internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Our school seeks to provide the right balance between controlling access, setting rules and educating students for responsible use.

We have;

- Installed and developed an intra school TV and radio station.
- A Virtual Learning Environment (eSchools).
- Run sessions for children, staff and parents on E-Safety.

This year we have aspirations to;

- Continue to develop the school website
- Run more sessions for children and parents on E-Safety

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- A well thought out approach regarding how to develop E-Safety guidance within the school's curriculum.
- Identified opportunities to ensure that we support families with the challenges relating to E-Safety in the digital age (family workshops, web-links etc).
- Secure, filtered broadband from Wirral Council's Network;
- A school network that complies with the National Education Network standards and specifications.

1.2 E-Safety and the Legal Issues

E-safety should be applied to protect children, staff and all members of our school community. Our School's e-Safety Policy replaces the Internet Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is a criminal offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children. In addition there are many grey areas for schools to consider regarding communication of social network sites, storage of data etc.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this school ensures that;

- It has effective firewalls and filters on our school network.
- Ensures that e-safety responsibilities are clearly communicated to all members of our school community.
- That our Acceptable Use Policies are fully enforced for children, staff and visitors.
- Ensures that our procedures are consistent with the Data Protection Act (1998)

Learning and Teaching in the Digital Age

The school uses wireless laptops and iPads and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology appropriately and safely.

2.1 Why the Internet and digital communications are important

Mobile Communication equipment and the Internet are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. We also recognise that children are actively engaged with digital communication form an early age. It is part of their lifelong learning experiences and habits. We have to embrace that opportunity. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

In addition use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Encouraging responsible use of the Internet and digital communication.

1. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is arranged through local authority provision and the school's network arrangements with RM. Only sites approved by the head teacher will be allowed to override the filter.

2. Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication.

3. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

4. Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.

5. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

6. Pupils will be shown how to publish and present information to a wider audience safely and responsibly.

2.3 Pupils will be taught how to evaluate Internet and other digital communication content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet or other digital content including messages, e-mails and texts. Whilst we cannot promote the use of social networking sites,

we must also ensure that our children know how to manage the risks and dangers associated with these activities.

Managing Digital Access, Communication and Content

All Internet accessed is managed by the school. Individual users should only access the Internet through their username and password. The school recognises that password protection is vital element of promoting e-safety.

The school will ensure that permission for access and use of any content including photographs and video is fully explained and sought on admission to the school.

3.1 Information system security

- School ICT systems security will be reviewed regularly. This will be part of the liaison between the Headteacher, School Business Manager and Hi-impact.
- Virus protection will be updated regularly as part of the school's Service Level Agreement with the Local Authority.
- Security strategies will be discussed with the Local Authority.

3.2 Managing filtering

- The school will work with Wirral Local Authority and other National Bodies to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator Mrs Morris.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.3 E-mail

- Pupils may only use their school approved e-mail account (eSchools) on the school system. All use of other e-mail accounts are prohibited.
- Staff should only use school approved e-mail accounts at work. Clear guidance for what constitutes professional use of e-mail is included in the Acceptable Use agreements. However, we are absolutely clear that staff cannot use e-mail to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

3.4 Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or a Senior member of staff.

- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.5 Publishing pupil's images

- Photographs that include pupils will be selected carefully. The school will always risk assess/review photographs for possible abuse.
- Names or any other personal details will never be published alongside photographs.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories Guidance @ Children, Families, Health and Education Directorate page 6 June 2008

3.6 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. The school will use the Virtual Learning Environment to teach children about social interaction and communication on the Internet. This should be carefully managed. All staff will seek the approval of the head teacher before using any sites with children. An example may be moderated social networking sites, e.g. SuperClubs Plus
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Staff are fully informed of their responsibilities regarding the use of social networking sites such as Facebook. At Eastway Primary we have agreed that it is good practice to separate professional and personal commitments. Therefore the following groups should not be allowed as contacts and friends on social networking sites;
  - **Ex pupils or current pupils** - the context of teacher to pupil relationship is not suitable for social networking.
  - **Parents** - We believe that it is unfair on parents and staff to complicate the professional relationship that exists within school through the use of social networking sites. It is both inappropriate and open to abuse.
- All staff are also aware that they could face charges of gross misconduct if they use social networking platforms to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.

- Staff are also aware that they are responsible for the security protocols regarding any social networking accounts. This is a professional responsibility.

NUT Cyber-Safe guidance states all staff should;

- not post information and photos about themselves, or school-related matters, publicly that they wouldn't want employers, colleagues, pupils or parents to see;
- keep passwords secret and protect access to accounts;
- not befriend pupils or other members of the school community on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils and let school management know if they decide to do this.)

NASUWT guidance states;

- To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly.
- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your school.

As a minimum, NASUWT recommends the following:

Privacy Setting	**Recommended security level**
Send you messages	Friends only
See your friend list	Friends only
See your education and work	Friends only
See your current city and hometown	Friends only
See your likes, activities and other connections	Friends only
Your status, photos, and posts	Friends only
Bio and favourite quotations	Friends only
Family and relationships	Friends only
Photos and videos you're tagged in	Friends only
Religious and political views	Friends only
Birthday	Friends only
Permission to comment on your posts	Friends only
Places you check in to	Friends only
Contact information	Friends only

- Always make sure that you log out of Facebook after using it, particularly when using a machine that is shared with other colleagues/students. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "Clear Chat history" in the chat window).
- Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see.

Conduct on social networking sites

- Do not make disparaging remarks about your employer/colleagues. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Act in accordance with your employer's information technology (IT) policy and any specific guidance on the use of social networking sites. If your school/college encourages the positive use of social networking sites as part of the educational process, they should provide clear guidance on what is considered to be appropriate contact with students. Having a thorough policy in place will help staff and students to keep within reasonable boundaries
- Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. If you face disciplinary action as a result of being tagged, contact NASUWT immediately.
- Parents and students may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.
- If you have any concerns about information on your social networking site or if you are the victim of cyberbullying, you should contact your NASUWT Regional Centre immediately.
- Do not publish your date of birth and home address on Facebook. Identity theft is a crime on the rise with criminals using such information to access to your bank or credit card account.
- Be aware of what monitoring, if any, may be carried out by the school/college. Full details of this should be detailed in the IT policy.
- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click "Privacy Settings". Under "Applications and websites" click "edit your settings". Scroll down to "instant personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation

This guidence is applied through the Local Authority's policy on the agreed use of social networking sites and the school's acceptable use and E-Safety code of conduct. All staff and visitors including students have to sign these when they join our staff team (see appendices 3 and 10)

3.7 YouTube

Youtube is a video sharing website that allows anyone to watch videos for free. Registered users can also upload videos for free. As staff we recognised that Youtube videos can add considerably to classroom practice, however we know that due to the broad spectrum of videos available not all content is suitable for classroom use. Therefore only videos which have been watched in their entirety by a staff member may be shown. Links to videos which have not previously screened must never be clicked, even when suggested as an alternative. Youtube videos may be embedded in class home pages on the Eastway eschools website which will allow our pupils to access videos without external links. Pupils will never be allowed to access Youtube without supervision. Staff are encouraged to regularly remind pupils about the positive and negatives attributes of using a site such as Youtube and should make clear that if anything that is seen which makes the child feel uncomfortable the screen

should be minimised (not shut down) and a responsible adult informed. When a report is made to a member of staff the time, date, location, child's name and website URL should be noted in the E-Safety incident log, along with other relevant information. The staff member must report the incident to the child's parents/carers and a senior member of staff.

3.8 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security. Video conferencing for pupils can only take place under the direct supervision of a member of staff. At Eastway Primary we will only use webcams for specific projects and full consent will be sought before children participate in these. Examples may be conferencing with another school in India.
- All software for webcam use will be password protected (Skype etc).
- Best practice recommends that schools always seek consent from parents for any video-conferencing. **See appendix 12**

3.9 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. For example mobile devices are allowed in school for children in years 5 & 6 but these are stored in a secure classroom based locker. Staff are allowed to have mobile devices in school but these must not be used during working hours except for school or emergency based communication in office areas or the staffroom and PPA room (see appendix 11)
- The senior leadership team should note that technologies such as mobile devices with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Personal mobile devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile devices is not allowed. **See mobile phone policy in appendix 11 for further details.**
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location. They can be used in school but NEVER for online gaming or internet access.
- Staff will be issued with a school mobile phone where contact with pupils is required or school camera to capture photographs of pupils. Staff must not take photographs on their personal phones. Guidance @ Children, Families, Health and Education Directorate page 7 June 2008. **See mobile phone policy in appendix 11 for further details.**
- The appropriate use of Learning Platforms will be discussed annually.

3.10 Protecting and storing sensitive data including images

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;

- All laptops must be password protected. Work laptops cannot be used for the storage of any inappropriate material.
- Photographs in DropBox should only be accessed in school and should be moved into the school media storage folder and deleted from the device also.
- All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.
- Photographs cannot be stored on personal laptops. The only exceptions are finger-tips E-Profile data and the archive stored by the head teacher.
  No data or images can be transported out of the school without the device being approved or password protected.

3.11 Use of Photographs

The Data Protection Act 1998 affects our use of photography. This is because an image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years (or the child him or herself if deemed competent from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings for purposes beyond the school's core educational function. (E.g. school web sites, school productions). At Eastway Primary we seek permission for all photography and video use.

There will also be times where the school will be carrying out off-site activities e.g. activity holidays or educational visits. Our guidelines are created to make sure that all images are taken appropriately by both adults in the school and children taking part in visits.

For both school / setting and other events which are photographed for publicity purposes additional consent should be sought from the child's parent/guardian or the child and kept on file covering all cases where images of children are to be published beyond the parameters of school use.

Where children are 'Looked After' schools must check consent on the corporate parent's behalf with the social worker and there may be other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child's security is known by the class teacher to be at stake, indicating the need for extra care.

Consent gained for photographs or videos may not extend to webcam use, so it is important to check, when introducing such technology, the status of existing consent for pupils or models.

Consent is sought for the whole time that children are at Eastway Primary. Parents retain the right to withdraw consent at any stage, but they need to do so in writing.

3.11a Planning photographs of children

Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.

- Where possible, use general shots of classrooms or group activities rather than close up pictures of individual children.

- Use images of children in suitable dress, and take care photographing PE events to maintain modesty, using team tracksuits if appropriate for example. Photographs should not be taken of swimming pool based events.

- Remember to include images of children from different ethnic backgrounds in your communications wherever possible, and positive images of children with disabilities to promote your school as an inclusive community, and to comply with the Disability Discrimination Act.

- Decide whether parents and visitors will be permitted to take photographs of the event. This must be authorised.

3.11b Identifying and children young people

If the pupil is named, avoid using their photograph. If the photograph is used, avoid naming the pupil.

It is our policy that;

- You use the minimum information. Ask yourself whether it is really necessary to accompany a picture with the pupils' names, the year group, or the school.

- When ***fully*** naming pupils in any published text, whether in the school's brochure, website, or in the local press, avoid using their photograph, unless you have parental consent to do so.

3.11c Using photographs of children supplied by a third party

When using third parties, it is our school's responsibility to check that the adults are aware of the school protocols. In addition we would expect that the adult taking the images has a full CRB or is supervised when taking images by a member of the school's staff.

Children should never be left alone with a photographer.

Copyright does not apply to images for private family use. However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting his or her work and to control how other people use it. If you commission photographs for use at school/setting or work include in your contract that the school will own the copyright for items taken on your behalf.

3.11d Use of Images of children by the Press

(Please refer to the recommendations in section 3.10b above; 'Identifying Pupils')
There may be occasions where the press take photographs at school of pupils. If this occurs we will ensure that specific permission is sought from the parent about whether to agree to their children being featured in the press and whether their full name should accompany the photograph.

3.11e Videos

School will ensure that parental consent is in place before any child can appear in a video, Parents can make video recordings of nativity plays and other such events for their own personal and family use, as they are not covered by the Data Protection Act. (Please refer to section 3.10h).

3.11f Websites

Web use can be of particular concern to parents and staff because of the potential misuse of images by paedophiles. With digital photography there is the remote possibility that images of children could be produced, manipulated and circulated without the parents or children's knowledge. The dual concern which follows such a risk is that children might be exploited and a school or setting might be criticised or face legal action. Images on website can be made more difficult to copy by several measures - copy-protection, overlaying with a watermark, or published in low definition.

It is important to take care with identification and to respect parental views on the use of any photography of children on a website.

Increasingly adults and children are generating content for websites e.g. children and adults placing pictures on **Bebo, Myspace,** or **Facebook** web sites. It is therefore important that schools/organisations ensure that children, staff and parents understand the risks involved and are encouraged to adopt safe practice when generating content for school related websites.

This is included on our permission forms. Parents and staff are not allowed to share school images on any Internet sites.

3.11g Webcams

The regulations for using webcams are similar to those for CCTV (closed-circuit television). This means that the area in which you are using the webcam must be well signposted and people must know that the webcam is there before they enter the area, in order to consent to being viewed in this way. Children should be consulted and adults would need to consent as well as the parents of all the affected children.

In gaining consent, the school must tell the person why the webcam is there, what you will use the images for, who might want to look at the pictures and what security measures are in place to protect access.

3.11h Parental right to take photographs and videos

We want parents to have the opportunity to record school events safely and responsibly.

We will allow recording, unless we feel that the images created may be inappropriate (for example a swimming gala, gymnastics display etc). We also have to ensure that consent is gained for all children taking part.

Parents are not covered by the Data Protection Act 1998 if they are taking photographs or making a video recording for **their own private use**. The Act does not, therefore, stop parents from taking photographs or making video recordings at school events, such as nativity plays or other such performances.

Parents are not permitted, however, to take photographs or to make a video recording for anything other than their own personal use (e.g. with a view to selling videos of a school event). Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent the Data Protection Act 1998 would be breached. **The consent form attached reminds parents of this fact**.

3.11i Images taken by young people

Children do have permission to take photographs on days out and residential trips etc. We will ensure that children understand that photographs must be responsible and not taken in private places. For example in bedrooms or toilets.

3.11j Use of Mobile Phones

Children are not allowed to use mobile phones in school. We allow children to bring mobile phones to school must these must be locked in their class safe.

Staff are not allowed to video or take photographs of children using mobile phones as the data is not easily transferrable and may breach our obligations under the Data Protection Act.

Visitors are also informed of this as part of our safeguarding statement.

Parents can use them for recording only based on the guidelines above.

4.1 Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' (see Appendix 3) before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- All Parents/Carers will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' (see Appendix 7) before being allowed to access the internet from the school site. This includes governors, Friends of Eastway visitors, student teachers etc.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor LA can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

4.3 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 head-teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Officer to establish procedures for handling potentially illegal issues. Children, Families, Health and Education Directorate page 8 June 2008

4.4 Community use of the network and Internet

- Through extended schools use and partnership with other organizations their will be wider community use of the school's network. The school will liaise with local organisations to establish a common approach to e-safety.
- All consent forms must be used for these groups.

Communicating the E-Safety Policy

5.1 Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

5.3 Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the school e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Appendix 1: **Agreed Staff Code of Conduct to promote E-Safety and Responsible Use**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional use.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school. I also understand my responsibilities regarding the use of photographs and videos and how to store these.

I understand that school information systems may not be used for private purposes without specific permission from the head teacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

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 install any software or hardware without permission.

I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. I understand that images of children from school cannot be stored on laptops.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.

I will ensure that electronic communications with pupils and parents including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I fully understand my professional responsibilities, if I chose to use Social Networking Sites.

I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information 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.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed:_____ Date: _____

Think Then Click!

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click!

E-Safety Rules for Key Stage 2

At Eastway Primary School we;

- We ask permission before using the Internet.
- We only use websites that an adult has chosen or approved.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We do not use mobile phones in school.

Appendix 6 – **Permission Letter for Network and Internet Use**

Eastway Primary School

E-Safety Rules Consent Form

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Our E-safety policy is available from the school office and is published on the school's website.

Pupil:	***Year Group:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

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 rule that photographs will not be accompanied by pupil names.

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.

Signed:	***Date:***

Please print name:

Please complete, sign and return to the School Office

Appendix 7: **Consent Form for Visiting Adults Using our Network and Internet Access**

All adults have to be responsible when using information systems. As visitors to schools, adults have to be aware that their activities must be related to education or their role within the school (PTA administration, family learning etc). Any abuse of this privilege could result in access being removed. In cases where the school feels that either their pupils or staff have been placed at risk, this could lead to the incident being reported to the police.

All visitors should consult the school's e-safety policy for further information and clarification. This is available through the school office or the school's website.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional and educational use. It is not appropriate to use social networking sites in school.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.

I understand that school information systems may not be used for private purposes without specific permission from the head teacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

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 install any software or hardware without permission.

I will ensure that no files are removed from the school's network without the express permission of a senior member of the school's staff.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the Headteacher.

I will ensure that al e-mail communication is appropriate.

I will not access any inappropriate websites including social networking sites.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information 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.

I have read, understood and accept the Visitor's Code of Conduct for ICT.

Signed:_____ Date: _____

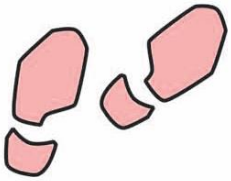
These rules help us to stay
safe on the Internet

Think then Click

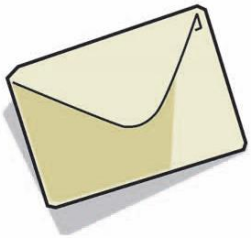
We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.



We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.

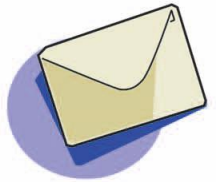
Think then Click

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.



We send e-mails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.

J. Barrett & H. Barton

POLICY ON THE USE OF SOCIAL NETWORKING WEBSITES (appendix 10)

The purpose of the policy is to provide clarity to all school staff on the use of any social networking website, e.g. Facebook, Twitter, Bebo and its implications in relation to future employment status i.e. disciplinary action and potential dismissal. The policy relates to any young person under 19 years of age, any 'looked after child' under the age of 21 years of age, and any young person with special educational needs under the age of 24 years of age.

Any member of staff can have an account on a social networking web site. However, it is the responsibility of the individual to ensure that anything placed on the social networking site is appropriate and meets the standards expected of professional teachers and school support staff.

NB *School employees who have their own social networking site may have contact with relatives or family friends. However all the requirements below would still apply to the use of Social Networking Websites.*

All school staff **must:**

- Demonstrate honesty and integrity, and uphold public trust and confidence in respect of anything placed on social networking web sites.
- Ensure that any content shared on any social networking web site, at any time, would be deemed as appropriate, i.e. staff are personally responsible for ensuring that any privacy settings meet this requirement.
- Ensure appropriate language is used, at all times, for any comments placed on social networking sites.
- Ensure that any comments and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.

All school staff **must not:**

- Have contact with current/ex pupils, or other children or young people where there is a relationship developed as part of their 'professional' role, e.g. music tutor, on any social networking website.
- Use social networking sites as a forum to make derogatory comments which could bring the school into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, local authority or the wider community.

Any breaches of this policy could result in disciplinary action and may result in your dismissal.

I understand and agree to adhere to the Policy on the Use of Social Networking Websites.

Signed	**Date**

This document has been developed and consulted on with Wirral Professional Teachers' Associations and Trade Unions

ASCL Association of School and College Leaders · ATL the education union · NAHT The Association for All School Leaders · NASUWT The Teachers' Union · NUT

Appendix 11 – Suggested form for seeking consent for Video Conferencing Projects

Dear Parents/Carers,

As part of our curriculum project on , the children will be using video-conferencing to communicate with . This is an exciting opportunity for your children. We also aim to teach children who to use video conferencing facilities safely.

For your child to take part in this project we need your permission.

2. Permission for children to participate in video conferencing projects		
Why is permission being sought?	**What are the school's responsibilities?**	
• **To help our children interact with different schools/settings using video conferencing facilities.**	• **To ensure that children only use video conferencing technology when they are supervised by a member of staff.** • **To ensure that all video conferencing software is password protected.** • **To ensure that we teach children how to use webcams and other technology safely and appropriately.**	
I give permission for my child to participate in the school's video conferencing project on		
	Signature	**Name**

Appendix 12 –

Eastway Primary School

Permission for my child(ren) to be filmed or photographed in school

Why is permission being sought?	What are the school's responsibilities?
• We use photography and video throughout the curriculum. Children may use it to film their play performance or take photographs for art ideas etc. • We also use photographs to celebrate achievements in school. • So that parents and children can film <u>authorised</u> school events (performances, sports days etc) for my personal use only.	• To ensure that all photographs/videos are appropriate and related to educational purposes. • To ensure that all photographs and videos are stored securely on password protected computers or encrypted memory pens. • Not to pass any photographs or video on to any 3rd party without parental permission. • To ensure that children's names are not printed next to photographs. • To ensure that all parents and carers are fully aware that photographs and videos taken at <u>authorised events</u> cannot be published on Internet sites including Facebook and other social networking sites**.**

I give permission for my child(ren) to be photographed or recorded as part of school activities.		
From time to time 3rd parties may ask for permission to use photographs to promote their activities. No children's names will published. I give permission for my child's photographs to be used.		
I request permission to take photographs and video recordings of my child(ren) at authorised school events (performances, sports days etc) and confirm these are for my personal use only and will not be shared on any Internet sites.		
	Signatures	**Name of child(ren)**

Please sign and return to the School Office

Appendix 13 –

Staff iPad usage agreement

Eastway Primary School provides Apple iPads for staff to enable them to carry out their job role more effectively. Please sign below to accept this iPad and agree to the following terms of use:

1. This iPad remains the property of Eastway Primary School and is loaned to you for use within your job role.
2. The iPad must remain in your possession, should only be used by you and should be securely stored when not in use.
3. All iPad use must fully comply with the Eastway Primary School e-Safety Policy and Data Protection Policy. Failure to do so may lead to disciplinary action.
4. The iPad is connected to your school network so may have access to the personal information of pupils. The iPad may also be used to store personal information such as picture and video images of pupils. This means you must fully comply with high standards of data protection.
5. This iPad is configured with certain restrictions in place. You must not try to make changes to the device that are passcode protected.
6. Loss or damage of the device should be reported to the Headteacher immediately. If necessary the device will be remotely locked or wiped.
7. You may connect the device to your personal Wi-Fi network in order to access internet-based applications such as Target Tracker.
8. Insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home **but excludes** theft from your car or from other establishments. Should you leave the iPad unattended and it is stolen you will be responsible for its replacement and may need to claim this from your own insurance company.
9. The iPad will be used in the classroom for pupil assessment recording. Remember that personal information might be accessible on the device and you must fully comply with high standards of data protection, therefore supervision of pupil use is required.
10. This iPad will be checked annually for safety and for compliance with school policies. Outcomes will be reported to the Headteacher.
11. If you leave the employment of the school the iPad must be returned in good condition to the Headteacher before your official leaving date.

iPad Model: ..... Serial No.: .....

Authorised by Headteacher: ..... Date: .....

Member of Staff: .....

I have read this agreement and fully understand that I need to adhere to all elements.

Received by Signature: ..... Date: .....