HOLY TRINITY
ENNISKILLEN

E-Safety Policy
And
Acceptable Use Agreement

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

- In ***Holy Trinity*** we understand the responsibility to educate our pupils in E-Safety (*Electronic Safety*) issues.

The Internet is an integral part of pupils' lives, both inside and outside school. There are ways for pupils to experience the benefits of communicating online with their peers, in relative safety. Child Exploitation and Online Protection (*CEOP*) resources are a useful teaching tool for all Key Stages looking at Internet safety and can be usefully incorporated into PDMU or ICT lessons.
If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

- All staff are encouraged to incorporate E-Safety activities and awareness within their lessons.

The CEOP link is available on all MySchool desktops.

Key concerns with using the internet

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons

Children should be taught:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details.
- That they should never meet alone anyone contacted via the Internet.
- That once they publish information it can be disseminated with ease and cannot be destroyed.

Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying should be considered within the schools overall anti-bullying policy and pastoral services as well as the E-Safety policy.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.

- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet.
Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.
Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.
Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children should be taught:-

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

Roles and Responsibilities

The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school.

The Principal/ICT Co-ordinator update Senior Management and Governors with regard to E-Safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service.
- Children are provided with technology in school and so they are not permitted to bring in their own devices to access the internet in school.
- No filtering service is 100% effective; therefore all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

- The school C2k system will block access to social networking sites.

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children or parents as 'friends' if they use these sites.

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website/Newsletter. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Parents will be reminded prior to any group performance that any photos/videos taken are not to be published in any public domain.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Community Use of School ICT Resources

- The school's ICT facilities are used as a community resource under the Extended Schools programme.
- Users are issued with separate usernames and passwords by C2K.
- They must also agree to the school's Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

Policy Decisions:

Authorising Internet access

- These E-Safety rules will be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's E-Safety rules and within the constraints detailed in the school's E-Safety policy.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network systems.

Handling E-Safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the E-Safety incident logbook.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communicating the Policy:

Introducing the E-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week.
- Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the **Thinkuknow website.**
- Pupils will be informed that network and Internet use will be monitored**.**
- There are various pupil resources available such as:

Signposts to Safety (primary and secondary versions)

Key Stage 2- 4
KidSMART
Know IT All for Schools
ThinkUKnow
Childnet's Sorted website

.

Monitoring and review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness regularly. They will do this by liaising with the ICT Co-ordinator and Designated Child Protection Co-ordinator.

ICT Code of Safe Practice for Staff
E-Safety Rules

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address or username & password to pupils.
- Any documents which need to be shared among staff should be saved in **Staff Resources**, NOT Shared Resources or Public.
- I will only use the approved, C2k, secure e-mail system for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the school Principal
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or principal.
- Images will not be distributed outside the school network without the permission of the parent/ carer or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school

Signature …….……. Date ……

Full Name ……....(printed) Job Title . . . . . .

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of or with their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- The school will communicate relevant E-Safety information through newsletters and the school website.

- Parents should remember that it is important to promote E-Safety in the home and to monitor Internet use.

  - Keep the computer in a communal area of the home.
  - Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones, tablets and kindles.
  - Monitor on-line time and be aware of excessive hours spent on the Internet.
  - Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
  - Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
  - Discuss the fact that there are websites/social networking activities which are unsuitable.
  - Discuss how children should respond to unsuitable materials or requests.
  - Remind children never to give out personal information online.
  - Remind children that people on line may not be who they say they are.
  - Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
  - Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Safety Rules for Children

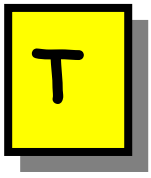
Follow these SMART TIPS

Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees.

ICT Code of Safe Practice
(Primary Pupils)

E-Safety Rules

- I will only use ICT in school for school purposes.
- I will not bring in any devices from home to access the internet in school.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Parental Agreement / Consent Letter

Dear Parent / Carer

As part of Holy Trinity Primary School's Information and Communications Technology programme, we offer pupils supervised access to a *filtered* Internet service provided by C2k. Access to the Internet will enable pupils to explore and make appropriate use of many web sites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However in spite of the tremendous learning potential, you should be advised that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service provider C2k has installed filtering software which operates by blocking thousands of inappropriate web sites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter.
Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact a member of staff.

We also require your consent for the use of photographs/video files for use in the school website and newsletter.

✂---

Signatures

We have discussed this and ……………………………………..........(child's name) agrees to follow the eSafety rules and to support the safe use of ICT at Holy Trinity Primary School.

Parent / Carer Signature: …….…………………….………………………… Date: ……………

Child's signature: ……….…………………….……………………………….. Date: ……………

We consent to the use of photographs/video files for use in the school website and newsletter.

Parent / Carer Signature: …….…………………….………………………… Date: ……………

Sample Posters

Key Stage 1

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.

B. Stoneham & J. Barrett

Key Stage 2

Think then Click

These rules help us to stay safe on the Internet

- We ask permission before using the Internet.

- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.

- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.

- We send e-mails that are polite and friendly.
- We do not open e-mails sent by anyone we don't know.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not use Internet chat rooms.