TOREAGH PRIMARY SCHOOL

E-Safety Policy
And
Acceptable Use Agreement

Date: September 2019

Review date: September 2022

Achieving, Believing, Caring

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

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.

In Toreagh Primary School, we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Key Concerns are:

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 or
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information it can be disseminated with ease and cannot be destroyed.

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 which share personal details, such as name, address, telephone number.
- Not to order online products without adult consent.

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.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. 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.

Writing and Reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by the Senior Management Team, Staff and Board of Governors. The e-Safety policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons. Each term, every class teacher reminds their group of children of how to keep safe online and reinforce the rules we have of using the internet in school. Current issues are discussed, if appropriate, during school assembly and/or class activities.
- All pupils take part in class activities during Safer Internet Day.

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of 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 will contain useful information and will link to sites like CEOP's thinkuknow, Childnet and the NSPCC and O2 page.
- The school will communicate relevant e-Safety information through newsletters, brochures and the school website.

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

- Keep ICT equipment 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.
- 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. Eg. turn the screen away from themselves and go and tell the adult who is caring for them at that moment.

- 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.

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, as part of the e-Safety curriculum and during Safer Internet Day.

- 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 Childlinet.

- The school Internet access is filtered through the C2k managed service.
- 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 taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- 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 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 a trusted friend/adult.
- School staff will not add children as ‘friends’ if they use these sites.

Mobile Technologies:

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils’ personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile devices/phones in school.
- Staff should not use personal mobile phones during designated teaching sessions.

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. 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.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also 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.

- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

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, MIS 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 and recorded by the ICT Co-ordinator. This will also be discovered through the use of Securus software.
- 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.
- Pupils and parents will be informed of the complaints' procedure.

Communicating the Policy:

Introducing the e-Safety Policy to pupils

- e-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of every term. 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/Safer Internet Day/Look After Yourself Week.
- Pupils will be informed that network and Internet use will be monitored**.**

.

Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop and/or iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

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 annually. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

E-Safety - Useful Websites

For Children

www.thinkuknow.co.uk includes sections for teachers, parents, children

www.kidsmart.org.uk – includes sections for teachers, parents

For Parents/Carers

www.childnet-int.org/kia/parents/
www.kidsmart.org.uk/parents
www.bbc.co.uk/webwise/
https://www.nspcc.org.uk/what-we-do/about-us/partners/nspcc-o2-online-safety-partnership

Safety Rules for Children

Follow These SMART TIPS when using the internet

S

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

M

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.

A

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.

R

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!

T

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

Toreagh Primary School

ICT Code of Practice Agreement for Foundation Stage Pupils and Parents

Toreagh Primary School has access to computers, laptops, a set of iPads and Internet access to help our learning. These resources are filtered and controlled by C2K. No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult. This filtered system enables staff and pupils to share and store materials electronically and to access a limited number of internet sites. Class rules are clearly displayed and discussed regularly with the children to ensure we stay safe when using ICT resources.

In school,

- **I will access the system with my login and password.**
- **I will take care of all ICT equipment including workstations, laptops and iPads.**
- **I will not access other people's work without permission.**
- **I will only use the designated computers and Ipads for school work and homework.**
- **I will not bring in software or pen drives/disks/CDs into school without permission.**
- **I will ask permission from a member of staff before using the Internet or printing.**
- **I will ask for help from a teacher or a suitable adult if I am not sure what to do or if I think I have done something wrong.**
- **I will tell a teacher or suitable adult if I see something that upsets me on the screen.**
- **I know that the ICT rules are there to keep me safe and that if I don't follow these I might not be able to use a computer, laptop or iPad.**

Signed by child ______________________________

Signed by parent/guardian ________________________

Date _______________________________

ICT Code of Practice Agreement for
Key Stage 1 Pupils and Parents

Toreagh Primary School has access to computers, laptops, a set of ipads and Internet access to help our learning. These resources are filtered and controlled by C2K. No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult. This filtered system enables staff and pupils to share and store materials electronically and to access a limited number of internet sites. Class rules are clearly displayed and discussed regularly with the children to ensure we stay safe when using ICT resources.

In school,

- **I will access the system with my login and password, which I will keep secret.**
- **I will not access other people's files without permission.**
- **I will only use the designated computers and iPads for school work and homework.**
- **I will not bring in software or pendrives/disks/CDs into school without permission.**
- **I will ask permission from a member of staff before using the Internet or printing.**
- **I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.**
- **I will report any unpleasant material or messages that I receive to my class teacher or responsible adult.**
- **I understand that the school may check my computer files and may monitor the Internet sites I visit.**
- **I will never give out personal information (including name, address, name of school etc..) usernames or passwords.**
- **I know that the ICT rules are there to keep me safe and that if I don't follow these I might not be able to use a computer, laptop or iPad.**

Signed by child

____

Signed by parent/guardian

____

Date

____

Toreagh Primary School

ICT Code of Practice Agreement for
Key Stage 2 Pupils and Parents

Toreagh Primary School has access to computers, laptops, a set of ipads and Internet access to help our learning. These resources are filtered and controlled by C2K. No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult This filtered system enables staff and pupils to share and store materials electronically and to access a limited number of internet sites. Class rules are clearly displayed and discussed regularly with the children to ensure we stay safe when using ICT resources.

In school,

- **I will access the system with my login and password, which I will keep secret.**
- **I will not access other people's files without permission.**
- **I will only use the designated computers and iPads for school work and homework.**
- **I will not bring in software or pen drives/disks/CDs into school without permission.**
- **I will ask permission from a member of staff before using the Internet or printing.**
- **I will only e-mail people I know, or my teacher has approved.**
- **I will not open e-mails sent by someone I don't know.**
- **The messages I send will be polite and responsible.**
- **I will not give my home address or telephone number, or arrange to meet someone.**
- **I will report any unpleasant material or messages that I receive to my class teacher or a responsible adult.**
- **I understand that the school may check my computer files and may monitor the Internet sites I visit.**
- **I will not use Internet chat-rooms in school.**
- **I will never give out personal information (including name, address, name of school etc..) usernames or passwords.**
- **I know that the ICT rules are there to keep me safe and that if I don't follow these I might not be able to use a computer, laptop or ipad.**

Signed by child

____

Signed by parent/guardian

____

Date

____

TOREAGH PRIMARY SCHOOL

Acceptable Use Agreement
For Staff

The computer system, iPads and ICT equipment is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's ICT and Esafety Policies have been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Enabling contact with pupils on social media websites is forbidden.
- Personal mobile phones should not be used in the classroom during class time.
- Personal tablets, laptops, Ipads or other ICT equipment should only be used in school after approval from ICT Coordinator and Principal and that they have been approved safe by electrical maintenance contractors approved by EA.
- If school owned devices (laptops or iPads) are taken home, careful storage and usage of them is essential.

Name		
Date		**Signed**

Toreagh Primary School
Teachers iPad Policy - School Supplied

Should the school supply an iPad for your teaching use, you agree the following:

• Use of the iPad should be considered the same as any other technology tool provided by the school.

• To abide by the schools Internet AUP with regard to iPad usage.

• All 'Apps' to be installed in the device will be discussed and approved by the ICT Coordinator prior to downloading.

• To ensure that all apps meet with the requirements of the schools Internet and ESafety AUP.

• To inform the ICT Coordinator of any apps that do not meet said requirements and remove them from your device.

• If there is a four-digit security PIN on the device, provide this on demand to the school management team

• To ensure that the security PIN of your device is held only by you and not divulged to pupils.

• To use only an account in the name of the school with your school email address for all App purchases.

• To not use the device to store personal documents such as video or audio material other than that which is directly related to your school needs.

• To not install any apps that may be considered only for your own personal use, or could be deemed not suitable for the classroom.

• Use of the camera only permitted in line with the whole school Safeguarding Policy.

• In the case of loss, theft or other damage occurring outside of school, to repair, replace or make good the iPad to its original state.

• That you will not sync or attach the iPad to your home or personal computer.

• You will not remove profiles or restrictions placed on the device.

• You will not 'jailbreak' the device. (ie. Hacking it to free it from Apple restrictions)

• To purchase and provide a case suitable to protect the iPad for general day to day school use.

• To not allow any pupil to use the iPad for any purpose except for curricular purpose under a controlled environment in the presence of a member of staff.

Name		**Ipad Serial No.**
Date		**Signed**