2024

ANAHILT
Primary School

E-Safety and the Acceptable Use of the Internet Policy

Policy Written by SMT

Reviewed: April 2025 **Next Review Date: April 2026**

E-Safety and Acceptable Use of the Internet

Introduction:

E-Learning is learning that is made possible and supported through the use of Information and Communications Technology (ICT) in school and at home. Whatever the technology being used by the individual learner, it enhances their educational experiences and supports lifelong learning. The staff of Anahilt Primary School believe that ICT is a valuable tool for teaching and learning.

At Anahilt, our vision is to prepare pupils for the challenges of a rapidly developing and evolving technological world. We recognise ICT as a core area of the curriculum through which we can enhance and extend learning and teaching. Our pupils should have an awareness of how to use technologies effectively for a wide range of purposes which add to the toolset they will need to be effective citizens and employees in the future.

Context:

This policy is based on and complies with DENI Circular 2007/1 on ***Acceptable Use of the Internet and Digital Technologies in Schools*** and DENI Circular 2011/22 on ***Internet Safety.*** The above circulars state that:

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Anahilt Primary School.

Care and Responsibility:

New technologies have become integral to the lives of children in today's society, both within schools and in their lives outside school. The Internet and other digital and information technologies are powerful tools, which open new opportunities for them. The use of these exciting and innovative tools has been shown to raise educational standards and promote pupil achievement.

Currently, the internet technologies children are using 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

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without consent or knowledge
- Inappropriate communication with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Illegal downloading or copying any copyright materials via the Internet or any mobile device
- The potential for excessive use which may impact on the social and emotional development and learning of our children

When using the Internet and other technologies children are vulnerable and may expose themselves to danger (knowingly or unknowingly). It is the duty of all stakeholders involved in a child's education to ensure that every child is safe and aware of the rules when using the Internet and Digital Technologies. As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any risks which may arise.

E-Learning in our School:

In Anahilt 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.

Anahilt Primary School has a managed computer service supported by C2K which provides us with computers and laptops in a designated computer suite. We also have Interactive Whiteboards in every classroom and a number of iPads. The school has a wireless network that allows children to access their individual documents, the Internet, and a local printer to support their learning.

E-Safety and Guidelines for the Acceptable Use of the Internet and Digital Technologies

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 online who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons.

Children will 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 easily shared 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 also 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 will 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 will 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.

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 online and to discuss problems. There are no totally effective solutions to problems of Internet Safety. Teachers, pupils and parents must be vigilant.

Peer on Peer Abuse:

We recognise the potential for online abuse between young people, outside of school hours. Our staff will remain vigilant to the signs of peer-on-peer abuse, including those between our pupils and young people who are not currently attending our school. Extra care should be taken where groups have mixed age, developmental stages and are attending other schools. When making contact with families, staff will ask about relationships between learners.

Risk Assessments in School:

The Senior Management Team (SMT) will perform risk assessments on the technologies used in school and review policies as new technology is introduced. New technologies will be assessed for their educational benefit and a risk assessment carried out before use. Pupils will be encouraged to develop safe online behaviour both in and out of school and know how to respond if they come across inappropriate material or situations.

Email Security:

The C2k Education Network filtering solution provides security and protection to C2k email accounts. It is advised that staff and pupils should use the C2k email system solely for school related work.

Memory Pens:

If a pupil brings a memory pen to use in school, it is the parent/carer's responsibility to ensure that it only has school related files saved on it.

Social Networking:

Staff will not communicate with parents/carers about school-based issues using social networking sites such as Facebook, Twitter, WhatsApp etc. If parents have a concern, they should contact the school office by email, telephone, in person or by letter.

Internet Security:

Staff and pupils accessing the Internet via the C2k Education Network are required to use their C2k username and password. Usernames and passwords must **NOT** be shared with anyone else. Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school Principal. Non C2k equipment will not be protected by C2k security software however, appropriate measures will be taken by the school to safeguard this equipment against security breaches.

General Use of ICT in the Northern Ireland education community will be in support of the aims and objectives of the Northern Ireland Curriculum

All users must:

- comply with all copyright laws
- limit their use of the Internet for school related purposes – examples of this include the use of email, the use of the Internet to investigate and research school subjects and staff using the Internet to further develop their professional development

- behave in an appropriate manner when communicating with others
- be aware that the use of the Internet in school is a privilege and not a right and this privilege will be withdrawn if it is misused
- respect the hardware and software that has been made available to them
- respect the work of others

Pupils:

- must not use another pupil's username and password.
- must not enter the folders or files of anyone else.
- working in pairs/groups should save their shared work onto individual memory pens.
- must be aware that teachers have the right to enter any pupil folders in their own class.
- will be made aware that the ICT Co-ordinator and Senior Management Team (SMT) reserve the right to enter any pupils' folders.
- must not use the Internet for unapproved purposes.
- are not permitted to bring in mobile phones or hand-held gaming consoles with downloadable capabilities to schools as they:
    - are valuable and may be lost or stolen.
    - can store images that are inappropriate.

Parents:

Parents should be aware that:

- in co-operation with staff, they should make their child(ren) aware of the rules and expectations within this document
- the access to the Internet provided to staff and pupils in school has limiting security features
- the use of the Internet in school is closely monitored by staff
- the use of ICT is complimentary to the teaching already done – i.e. the use of computers in the classroom is a tool
- no photographs of pupils will be available online without parents giving their permission
- photos used on the school website will not include full names
- pupils are not allowed to bring mobile phones to school on the grounds that Internet access becomes very difficult to police

Parents should also be aware that social networking sites
Facebook/Twitter/Snapchat/TikTok/WhatsApp etc adhere to a strict 'over 13s' age policy

Network administrators reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibility – they will respect the right to privacy whenever possible.

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 will update the Senior Management Team and Governors with regard to E-safety to ensure that all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

E-Safety Skills' Development for Staff

- All staff receive information and training on E-safety issues through the co-ordinator at staff meetings, when appropriate.
- 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.

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 will communicate relevant E-safety information through newsletters and the school Website, when relevant.
- The Safer Schools NI App is available to parents.

Parents should remember that it is important to promote E-safety in the home and to monitor Internet use. ***Good practice is as follows:***

- 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.
- Monitor online time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing and discuss with them what they are seeing and using on the Internet.
- Advise children to use the Internet in a sensible and responsible manner. Follow the SMART Rules. ***(See Appendices 1&2).***
- 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 online may not be who they say they are.
- Be vigilant and ensure that children do not arrange to meet someone they meet online.
- 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

Education of Pupils:

Educating pupils about Internet safety will be part of the ICT programme and usefully incorporated into PDMU when appropriate. Parents are encouraged to talk to their children about acceptable use of digital technologies. To support parents further, the school will invite appropriate professionals in from time to time to discuss Internet safety. Safety rules will be displayed in the ICT Suite.

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.
- Pupils are aware of the impact of online bullying (cyberbullying) 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 eg. parent/carer, teacher/trusted member of staff, or an organisation such as Childline.
- The school Internet access is filtered through the C2k managed service, although no filtering service is 100% effective.
- Use of the Internet is a planned activity.
- Pupils will be taught what Internet use is acceptable and what is not, and they will be 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.
- Children are taught to be *Internet Wise* by being made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

E-mail: (P6/7 ONLY)

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an 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.

Social Networking:

- The school C2k system will block access to social networking sites.
- Pupils and parents are advised that the use of social network platforms 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 may **NOT** use social network platforms in school or on school trips.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are asked to report any incidents of cyberbullying to the school.
- School staff will **NOT** add children as 'friends' if they use these sites.

Mobile Technologies:

- The use of portable devices such as memory sticks should only contain school related material. They should not contain photographs or pupils' personal data.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to bring personal mobile devices/phones to school.
- Staff should not use personal mobile phones during designated teaching sessions.
- iPads will only be used under the direction of a member of staff for a particular educational purpose.

Managing Videoconferencing:

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

Publishing Pupils' Images and Work on School Website

The school's website address is www.anahiltprimary.co.uk. As our website continues to grow, we intend to develop the existing **Photo Gallery Section** showcasing pupils' work as well as engagement in a variety of noteworthy activities, including special events and competitions. In addition, photographs are found in the **Class Pages Section** of the website. When posting photographs to the site we will ensure that:

- Written permission from parents/carers will be obtained before photographs of pupils are published. This consent form is considered valid for the entire period that the child attends this school.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not attached to any photographs on the school website.
- Pupils' work can only be published by outside agencies if parental permission is granted.

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 (***Appendices 3 & 4***) and abide by the school's E-Safety rules. (***Appendices 1& 2***). These E-Safety rules will be displayed clearly in the ICT Suite and individual classrooms.
- Access to the Internet will always be supervised. (P1-P5)
- 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. (***Appendices 3 & 4***)

- All staff must read and sign the Acceptable Use Agreement for Staff (***Appendix 5***) before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they must change regularly. Login details should not be shared with pupils or other staff.
- 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 Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

Handling E-Safety Concerns:

- Complaints of Internet misuse will be dealt with by the Principal.
- 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/illegal nature will be reported to the Designated Teacher/Principal and must be dealt with in accordance with the school's Safeguarding and Child Protection Policy.
- Incidents of pupil misuse of technology will be dealt with in accordance with the school's Positive Behaviour Policy.
- Cyberbullying will be dealt with in accordance with the school's Anti-Bullying Policy.
- Parents will be informed of the school's Complaints' Procedure (available on the school's website).

Other Related Policies:

- ICT Policy
- Social Media Policy
- Safeguarding and Child Protection Policy
- Positive Behaviour Policy
- Pastoral Care Policy
- Anti-Bullying Policy
- Curriculum Policies

Communicating the Policy:

Introducing the E-Safety Policy to Pupils

- E-Safety rules (***SMART Rules – see Appendices 1 & 2***) will be displayed in the ICT suite and discussed with the pupils at the beginning of September each year and revisited at the beginning of Terms 2 and 3. Specific lessons will be taught by class teachers at the beginning of every Term and at relevant points throughout the year e.g. during PDMU

lessons/circle time/anti-bullying week. Particular focus will be placed on E-Safety on "Safer Internet Day."

- Children are to sign the Acceptable Use of the Internet Agreement (***Appendices 3 and*** 4).
- Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety Policy

- All staff will adhere to the school's E-Safety Policy. The policy will be revisited on an annual basis as part of the school's Safeguarding and Child Protection refresher training programme.
- Staff will be asked to read & sign the Acceptable Use Agreement for Staff (***Appendix 5***).
- 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 are essential.
- A laptop 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.
- All teachers are encouraged to incorporate E-Safety into their activities and promote awareness within their lessons.

Parents and the E-Safety Policy

- The school's E-Safety Policy will be available for all parents to read on the school website. Paper copies will be available on request.
- Parents will be requested to read and sign the Acceptable use of the Internet Agreement form, following discussion with their child. (***Appendices 3 & 4***)
- Anahilt Primary School will seek to promote E-safety awareness within the school community, which may take the form of parents' information evenings, articles in the newsletter or links on the school website.

Guest Users

Parents and members of the community may use computer facilities within the school. They will be allocated a username and password for use in that session. This will provide access to the Internet and software available on the school network. They will not be able to save work onto the school network or access any school documents.

Any parent or member of staff who wishes to discuss this document should contact Mr A Smyth (Principal)

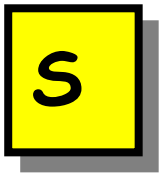
E-Safety Monitoring and Policy Review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator. This policy, supported by the school's Acceptable Use Agreement for staff and pupils, is to protect the interests and safety of the whole school community. It has been agreed by the Senior Management Team, staff and ratified by the Board of Governors.

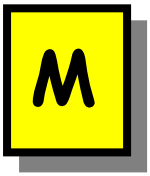
The E-Safety Policy, its implementation and effectiveness will be reviewed annually.

Appendix 1 (P3-P7)

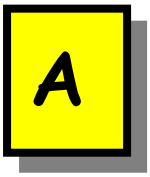
Be SMART to Stay Safe



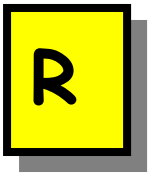
Secret - Always keep your name, address, mobile phone number and password private- It's like giving out the keys to your home!



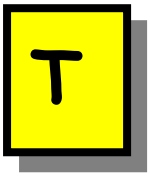
Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent/carer's permission, and when they can be present.



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



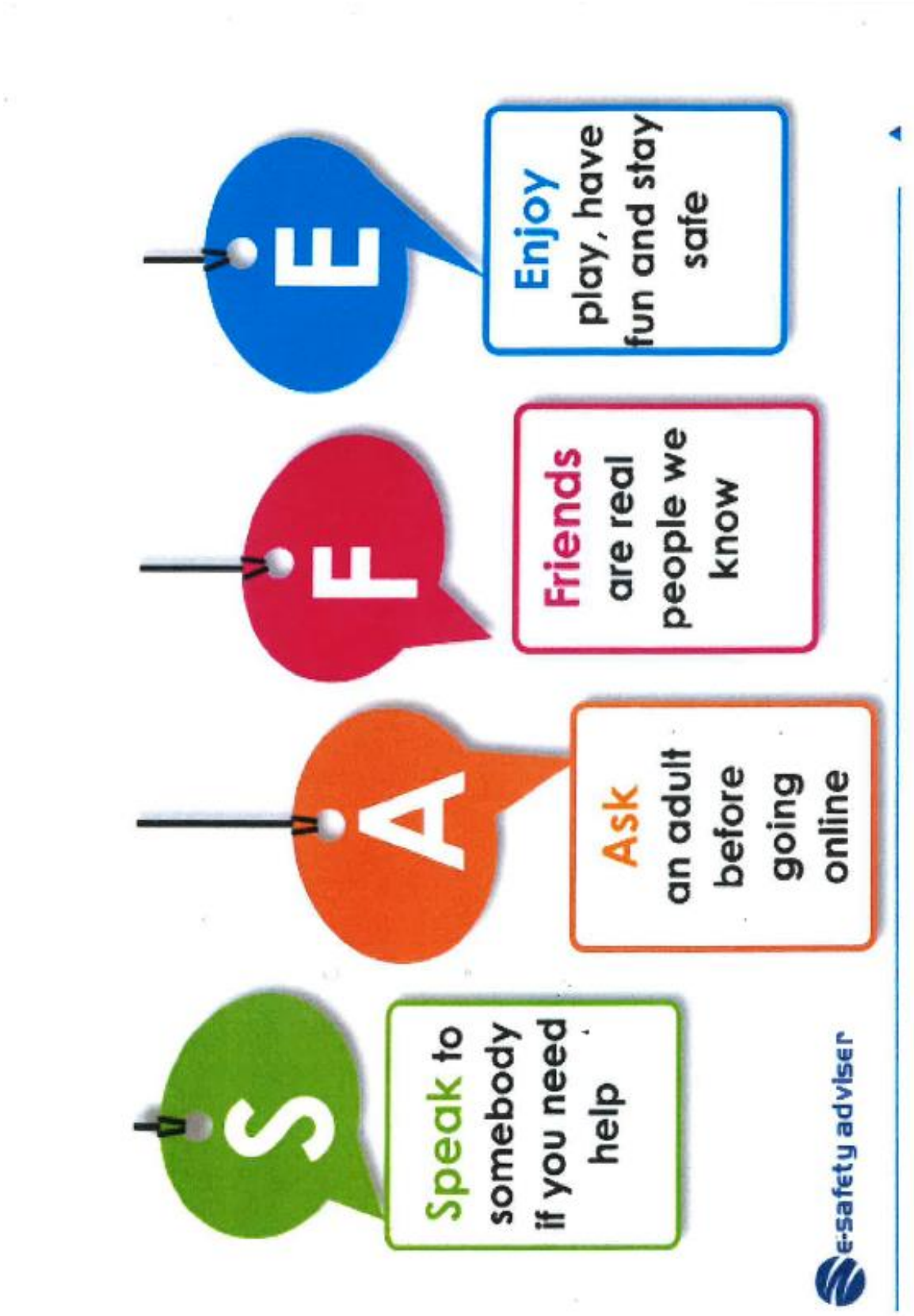
Remember, someone online may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



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

Appendix 2 (P1-P2)



Appendix 3 P5-P7

Anahilt Primary School

Rules for Acceptable Use of the Internet

Anahilt Primary School has installed computers, Interactive White Boards, iPads and Internet access to help us in our learning and understanding.
The rules below will help keep everyone safe and help us to be fair to others.

- I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission from a member of staff before using the Internet.
- I will use the Internet for research and school purposes only.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell the teacher immediately.
- I will not bring in a memory stick unless I have been given permission.
- I understand that the school may check my computer files, emails, and may monitor the Internet sites that I visit.
- I am not allowed to enter Internet Chat Rooms while using school computers.
- I will only send e-mails to my peers in school or to someone whom my teacher has approved. I will make sure that the messages are polite and responsible.
- When sending e-mail, I will not give my name, address or phone number or arrange to meet anyone.

I understand that if I deliberately break these rules, I may be stopped from using the Internet and my parents/carer will be informed.

I have read the rules with my parents/guardian. I will abide by the rules.

Pupil's Name: _____

Pupil's Signature: _____

I have discussed the above rules of acceptable use of the Internet with my child.

Parent/Guardian's Name: _____

Parent/Guardian's Signature: _____

Appendix 4 P3-P4

Anahilt Primary School

Rules for Acceptable Use of the Internet

Anahilt Primary School has installed computers, Interactive White Boards, iPads and Internet access to help us in our learning and understanding.

The rules below will help keep everyone safe and help us to be fair to others.

- I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission from a member of staff before using the Internet.
- I will use the Internet for research and school purposes only.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell the teacher immediately.
- I will not bring in memory sticks unless I have been given permission.
- I understand that the school may check my computer files, and may monitor the Internet sites that I visit.
- I am not allowed to enter Internet Chat Rooms while using school computers.

I understand that if I deliberately break these rules, I could be stopped from using the Internet and my parents/carer will be informed.

I have read the rules with my parent/Guardian. I will abide by the rules.

Pupil's Name: _____

Pupil's Signature: _____

I have read and discussed the above rules of acceptable use of the Internet with my child.

Parent/Guardian's Name: _____

Parent/Guardian's Signature: _____

Appendix 5

Anahilt Primary School

Acceptable Use of the Internet

in the workplace

Agreement for Staff

The computer system 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 Internet Access Policy has 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.

This covers school PCs, laptops, Ipads and Surface Pro PCs.

- 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-mails 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.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As e-mail can be forwarded or inadvertently 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.

Name: _____

Signature: _____ **Date** _____