DRUMAHOE PRIMARY SCHOOL

POLICY ON E-SAFETY

Drumahoe Primary School
Code of Practice for Safe and Effective Use of I.C.T. and e-Safety

What is e-Safety?

e-Safety is short for electronic safety. It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. e-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

e-Safety:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident on-line;
- is concerned with supporting pupils to develop safer on-line behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

When using the internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. **(See DENI Circular 2016/27).** Drumahoe Primary School will therefore make explicit to pupils – (**see Appendices 1& 3**) what is safe and acceptable and what is not. Drumahoe Primary School will ensure that all pupils understand how they are to use the Internet safely, effectively, appropriately and why the rules exist.

These issues will include:

- creating, retrieving, downloading, sending, copying, printing or displaying on-screen offensive messages or pictures;
- use of obscene or racist language;
- harassing, insulting or attacking others;
- damaging computers, computer systems or computer networks;
- violating copyright laws;
- using another user’s password;
- trespassing in another user’s folders, work or files;
- intentionally wasting resources (such as on-line time and consumables);
- using the network for unapproved commercial purposes.

The Code will balance the desirability of fully exploiting the vast educational potential of new technologies with providing safeguards against risks and unacceptable material and activities.

The scope of the Code will cover fixed and mobile Internet; technologies provided by the school (such as PCs, laptops, iPads, webcams and digital video equipment); as well as technologies owned by pupils and staff, but brought onto school premises (such as mobile phones, camera phones, personal digital assistants (PDAs), and portable media players). It will be made clear in this Code that the use of devices owned personally by pupils are subject to the same requirements as technology provided by the school.

The school requires that pupil/parent sign the use agreement (**see Appendices 1 & 2**) document as a means of demonstrating that policy has been communicated to all users. It will include doing anything outside of school and/or on-line, that may bring the school's name into disrepute. This will include posting derogatory information about teachers or the school.

However, understanding the issues and displaying safe effective practice is as important as having a written document and therefore, an education programme is an essential element of a 'Code of Practice'. Drumahoe Primary School will also ensure that all users are aware that the school tracks and records the sites visited, the searches made on the Internet and emails and messages sent and received by individual users.

In promoting awareness of best practice, pupils will:

- be involved in creating/reviewing the 'Code of Practice' through the Kids Forum;
- know how to identify and report any inappropriate use of technology;
- be aware that their on-line behaviour is tracked and recorded at all times;
- know the sanctions for misuse or abuse (ranging from suspension of the use of technology to involvement of the police and legal action in serious cases).

Parents ought to be made aware that when pupils use the C2K on-line learning environment whether in school or outside, they will be agreeing to certain terms and conditions of appropriate usage. These terms are available on the C2K Learning NI website.

e-Safety Team

This e-Safety policy has been developed by the E-Safety Team of Drumahoe Primary School which is made up of:

- The Principal (Mr McMaster);
- The UICT/ E-Safety Co-ordinator (Mrs Wheeldon);
- The Designated Teacher for Child Protection (Mrs Hegarty);
- The Designated Governor for Child Protection (Mrs P McClements)

The E-Safety policy will be reviewed annually, or in response to any significant new developments, threats or incidents, and will address the following:

1 Principles of our e-Safety policy;

2 Purposes of our e-Safety policy;

3 Practices of E Safety to include:

- Roles and Responsibilities;
- Policy Statements.

PRINCIPLES

New technologies have become integral to the lives of children and young people 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 up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. In Drumahoe Primary School we recognise the benefits that ICT can bring to teaching and learning and believe these benefits "outweigh the risks." However, as a school we endeavour, through our e-Safety policy, to meet the statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

A school e-Safety policy, in addition to our Acceptable Use of the Internet Policy should help to ensure safe and appropriate use.

The use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
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 an individual's consent or knowledge;
- inappropriate communication / contact 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;

- plagiarism and copyright infringement;

- illegal downloading of music or video files;

- the potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other school policies.

As with all other risks, it is impossible to eliminate those risks 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 these risks.

PURPOSES

Our purposes in having an e-Safety policy are:

- To safeguard our pupils and staff in the digital world so that they understand and use new technologies in a positive way;

- To educate our pupils about the risk as well as the benefits;

- To support pupils to develop safer on-line behaviours both in and out of school;

- To help pupils recognise unsafe situations and how to respond to risks appropriately.

PRACTICES - ROLES AND RESPONSIBILITIES

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The designated Governor for Child Protection has also taken on the role of UICT/E-Safety Governor. The role of the E-Safety Governor will include:

- liaising with the Principal and E-Safety Co-ordinator (Mrs Wheeldon);
- monitoring of the e-Safety incident logs;
- reporting to the Board of Governors, where necessary.

Principal & S.M.T.

- the Principal is responsible for ensuring the safety (including e-Safety) of members of the school community, though the day to day responsibility for e-Safety will be delegated to the E-Safety Co-ordinator (Mrs Wheeldon);
- the Principal and SMT are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-Safety roles and to train other colleagues, as relevant;
- the Senior Management Team will, when requested, receive monitoring reports from the E-Safety Co-ordinator;
- the Principal and SMT should be aware of the procedures to be followed in the event of a serious breach of e-Safety – see AUI Agreements **(see Appendices 1,2 & 4).**

- ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ensure that users may only access the school's network through a properly enforced password protection policy, in which passwords are regularly changed
- C2K are informed of issues relating to the filtering applied
- the C2K/school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person but that of all members of staff.
- that the ICT/E-Safety co-ordinator keeps up to date with e-Safety information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the principal, E-Safety Co-ordinator or class teacher

E-Safety Team

It is the responsibility of the members of the e-Safety Team to assist the e-Safety Co-ordinator with the production, review and monitoring of both the E-Safety policy and the filtering policy.

E-Safety Co-ordinator/Child Protection Co-ordinator

As sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults or strangers, potential or actual incidents of grooming, cyber-bullying, etc are child protection issues the E-Safety co-ordinator and the Child Protection Co-ordinator will work together to ensure the E-Safety of all.

The E-Safety Co-ordinator in Drumahoe Primary School is Mrs Wheeldon, supported by the Child Protection Co-ordinator, Mrs Laura Hegarty. They will, alongside the Principal:

- lead the e-Safety Team;
- take day to day responsibility for e-Safety issues and have a leading role in establishing and reviewing the school e-Safety policies / documents;
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place;
- provide training and advice for staff;
- liaise with relevant bodies;
- receive reports of e-Safety incidents and create a log of incidents to inform future e-Safety developments.
- report to other members of Senior Management Team.

Staff

The UICT Co-ordinator is kept informed and updated on issues relating to Internet Safety, attends appropriate courses and accesses advice and support through C2k.

Training and advice is disseminated to all teaching staff, classroom assistants and supervisory assistants as appropriate to ensure that all reasonable actions and measures are put in place to protect all users. This is carried out in liaison with the Designated Teacher & Deputy Designated Teacher for Child Protection.

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. The '**Acceptable Use Agreement'** is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of ICT. All members of staff are expected to sign this policy and adhere at all times to its contents (**see Appendix 4**). Members of staff are encouraged to use the Internet as a resource in teaching and learning. They use the service to support the aims and objectives of the Northern Ireland Curriculum, to conduct research, and for contact with others in the world of education.

All members of staff are expected to communicate in a professional manner. While normal privacy is respected and protected by password controls users may not expect files and messages stored on the network to be private as network administrators may review files etc. to maintain system integrity.

Guidelines for Staff (see Appendices 1, 3 & 4):

- Pupils accessing the Internet should be supervised by an adult at all times;
- Pupils are aware of the rules for the safe and effective use of computers/iPads; These rules are displayed in the ICT room and corridors and should be on display in each classroom. Rules should be regularly discussed with pupils and referred to when using computers/iPads;
- All pupils using the Internet have written permission and pupils from P3-P7 have signed the pupil agreement also;
- Equipment, websites, Apps and on-line content including video recommended for use by pupils should be checked beforehand by teachers to ensure that there is no unsuitable content and that material is age appropriate;
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the ICT Co-ordinator/Principal;
- In the interests of system security, staff passwords should only be shared with the Network Manager(s);
- Teachers are aware that the c2k system tracks all Internet use and records sites visited. The system also logs emails and messages sent and received by individual users;
- Staff are strongly advised to use only their C2k email account for school business;
- Teacher should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these;
- Photographs and videos of pupils should, where possible, be taken with school equipment and images should be stored on the school network accessible only by staff;
- School systems may not be used for unauthorised commercial transactions;
- Staff will read and sign the Staff User Agreement for Internet Access and also follow the guidelines contained in Staff Code of Conduct document.
- Staff iPads should never be put in front of children, These are for staff professional development use and may contain content that is not age appropriate for children to use;
- Staff should not download Apps on to school pupil iPads. This will be done by and with the consent of the UICT Co-ordinator.

Teaching and Support Staff:

- have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices;
- will avail of on-going CPD in relation to e-Safety;
- have read, understood and signed the school's Staff Acceptable Use Policy / Agreement (AUP/AUI) (**see Appendix 4**).
- will report any suspected misuse or problem to the Class Teacher, E-Safety Co-ordinator or Child Protection Co-ordinator, for investigation / action / sanction;
- use digital communications with pupils (email / Virtual Learning Environment (VLE) / etc) should be on a professional level only;
- ensure e-Safety issues are embedded in all aspects of the curriculum and other school activities;
- ensure that pupils understand and follow the school e-Safety and acceptable use policy (**see Appendix 1**).;
- will monitor ICT activity during class tasks or if supervising out-of-class activities;
- are aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- ensure that lessons where the use of the internet is pre-planned, pupils should, as far as possible, be guided to sites checked as suitable for their use;
- put processes are in place for dealing with any unsuitable material that is found when pupils research topics or for information on sites that have not been checked.

Parents / Carers

Parents will be advised that Drumahoe Primary School, through C2K, provides a filtered and monitored access to the Internet. Their attention will be drawn to the school's guidance and advice on its acceptable use.

We recognise the important role of parents / carers in ensuring their children understand the need to use the Internet or mobile devices in an appropriate way. They will be requested to read the regulations laid down by the school and sign a declaration of agreement. They will be responsible for endorsing their child's Using the Internet - Pupil Agreement (**see Appendix 2**) which will provide an opportunity for parents to discuss e-Safety issues with their child and links to appropriate websites will be provided.

Parents will be encouraged to use this guidance when allowing their children access to the Internet at home. Parents in P1 are asked to read our Acceptable Use Agreement on behalf of their child as part of the induction process. This is repeated in P3 when pupils are also asked to agree to and sign our Using the Internet Pupil Agreement and return it to school. Forms will be issued accordingly to new pupils.

For Parents:

The Code of Practice for Safe and effective Use of ICT and policies for use of Mobile Phones, Cyberbullying and Social Networking are available on the school website and from school on request.

Other literature and advice is also given to parents as appropriate and periodically workshops for parents are provided.

Appropriate and Acceptable Use of the Internet

The following on-line activities are to be encouraged –

1. Using Internet sites such as BBC School sites to access programs that help to reinforce, inform, challenge and extend learning.

2. Using the Internet to investigate and research school subjects, cross-curricular themes and topics related to social and personal development.

3. Using the Internet to develop ICT skills and general research skills.

4. Using e-mail and computer conferencing for communication between colleagues, between pupil(s) and teacher(s), between pupil(s) and pupil(s), between schools and industry.

N.B. In the Foundation and Key Stage 1 classes the Internet will mainly be used to consolidate and extend learning through interactive games and activities that have been carefully selected by the class teacher.

Inappropriate and Unacceptable Use of the Internet

The following on-line activities are not permitted;

1. Searching, viewing and/or retrieving materials that are not related to the aims of the curriculum.

2. Copying, saving and/or redistributing copyright protected material, without approval.

3. Subscribing to any services or ordering any goods or services, unless specifically approved by the school.
4. Playing computer games or using interactive chat sites, unless specifically assigned by the teacher.

5. Using the network in such a way that use of the network by other users is disrupted (for example, downloading large files during peak usage times; sending mass e-mail messages).

6. Publishing, sharing or distributing personal information about a user (such as home address, e-mail address, phone number, etc)

7. Any activity that violates a school rule.

8. Using another user’s password.

9. Use of obscene or racist language.

10. Harassing or insulting other users.

Advice to Parents

Teachers and Governors of Drumahoe Primary School will endeavour to ensure that the pupils in their care use the Internet responsibly, according to the policy of the school. They will guide the children towards appropriate materials and monitor on-line activities.

While in school pupils' access to the Internet will be through a filtered service ensuring that, as far as possible, unsuitable material will be barred.

Outside school it is parents' responsibility to provide guidance in their children's use of the Internet. Parents do not usually permit their children to view unsuitable television programmes, films, videos, etc, and the same precautions apply to their use of the Internet. However, appropriate use at home will be beneficial to children educationally, and will often be a valuable aid to both homework and school work. We would advise that this use is closely supervised to eliminate access to inappropriate material.

We would further advise that parents also provide a filtered internet service for their children's use thus greatly reducing the chance of accessing unsuitable sites.

Advice and Guidance for Parents:

- Discuss with your child rules for using the Internet and decide together when, how long, and what is meant by appropriate use.
- Know the web sites that your child visits.
- Talk to your child about what they are doing and learning.
- Encourage your child **not** to respond to any unwelcome, unpleasant or abusive messages, and to tell you if they receive such a message.
- Discuss with your child the importance of **not** giving out **any** personal identifying information in any electronic communication on the Internet or through other online environments
- Supervise your child's use of the Internet. It may be helpful to have the computer set up in a family room, if possible.

Pupils

- pupils in Primary 3-7 will be asked to read, agree and sign our 'Using the Internet Pupil Agreement' (**see Appendix 1**).Pupils are responsible for using the ICT in school in accordance with this Policy and will expected to sign the agreement to this effect before being given access to school systems. Parents of pupils in Years pupils in Years 3 – 7 will also sign the declaration (**see Appendix 2**) stating that they have discussed the Acceptable Use of the Internet with their child before signing the agreement;

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying;

- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions out of school, if related to the Drumahoe Primary School community.
- will take part in planned e-Safety activities.

Access to the Internet is a learning tool that is given to pupils who act in a responsible manner. Evidence of inappropriate use will be dealt with in accordance with the schools positive behaviour policy. Incidents of deliberate access to inappropriate materials by any user will be recorded by the UICT Co-ordinator in the e-Safety Incident Logbook.

Pupils will have the opportunity to take part in an Internet Proficiency programme which aims to help them develop safe and responsible behaviour when using the Internet and other interactive technologies.

Internet Safety Awareness

At Drumahoe PS we believe that alongside having written policies on e-Safety and Acceptable Use of the Internet and a Code of Practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use of the Internet as an essential element of the school curriculum. This education is as important for staff and parents as it is for the pupils.

For pupils:

Rules for e-Safety and using computers/iPads are discussed with pupils and are prominently displayed in the ICT room, corridors and classrooms. SMART tips **(see Appendix 5)** are also discussed with the children and displayed. These rules and tips are referenced at the start of any ICT activity.

Children will also take part in lessons and activities with a specific theme of on-line safety delivered through ICT and PDMU lessons, assemblies and the help of outside agencies and on-line resources such as CEOP and Childnet.

Pupils will also take part in activities for Safer Internet Day in February of each school year.

Community

If the wider community wish to avail of school ICT systems they too will be required to sign a the Acceptable Use of the Internet Agreement (**see Appendix 4**) before access to school systems is granted. This will be drawn up in consultation with the e-Safety Team.

Filtering of Non-Classroom 2000 systems and services

If the school chooses to access on-line services through service providers other than C2K, then it is responsible for ensuring that effective firewalls, filtering and monitoring software mechanisms are put in place. We will regularly review their filtering and blocking policies and procedures. Procedures for both blocking and unblocking sites will be clearly communicated to all staff members. Currently the school only uses the C2K system.

What is the Internet?

The Internet is an electronic highway connecting computers and individuals all over the world. The educational value of appropriate information on the Internet is significant.

However it also includes material that may be considered inappropriate to children’s needs in primary school, and may be racist, inaccurate, abusive, profane, sexually orientated or illegal.

C2K

All schools in Northern Ireland have access to the Internet, electronic mail and on-line computer conferencing through C2K. C2K has installed filtering software that operates by blocking inappropriate web sites and by barring inappropriate items and searches. However, it must be stated that no filtering service can be foolproof and so it is essential that users behave in a responsible manner according to the guidance given in the acceptable use of the resources, backed by these policy guidelines.

Location and Supervision

Access to the Internet for pupils is available on computers and iPads in the classrooms and the computer suite. These computers/tablets are in full view of people moving around these areas. Pupils’ use of the internet, at school, will be supervised and pupils will be reminded of what is considered acceptable. Pupils must be aware of what constitutes appropriate use, and of the school policy.

Health and Safety

Drumahoe PS has attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT Resources. Use of Interactive Whiteboards and Digital Projectors is supervised at all times. Children are given rules and guidelines for using iPads correctly.

Digital and Video Images of Pupils

Written parental permission has to be given to cover the use of photographs of pupils on the school website, printed or electronic publications, local press, promotional videos and the school Facebook/Twitter page.

To Minimise Risks:

- Group photos are used where possible with general labels and captions;
- The website, Twitter and Facebook pages do not include home addresses, telephone numbers, personal emails or any other personal information about pupils or staff;
- Digital and video images are, where possible, taken with school equipment;
- Images are stored on the school network, accessible only by staff.

Risk Assessments

21st century life presents dangers including violence, racism and exploitation form which pupils need to be constantly protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks – to become “internet-wise” and ultimately good “digital citizens”. Risk assessments are carried out on the technologies used within school to ensure we are fully aware of and can mitigate against the potential risks involved with their use. Our aim is to teach our pupils how to cope if they come across inappropriate material or situations online.

Sanctions and Dealing with Inappropriate Use

Incidents of technology misuse will be dealt with in accordance with the school's Positive Behaviour policy. Incidents of deliberate access to inappropriate materials by any user will be recorded by the UICT Co-ordinator in the e-Safety Incident Logbook.

Sanctions may mean the temporary suspension or withdrawal of privileges associated with internet access and use of technology.

Incidents involving child protection issues will be reported to the Designated Teacher for Child Protection and dealt with in accordance to our Safeguarding and Child Protection policies.

Staff misuse of the internet or digital technologies will be referred to the Principal.

Appendix 1

DRUMAHOE P.S.

Using the Internet
Pupil Agreement

I promise that I will use the Internet sensibly and will not use it for the following purposes

1. Searching, viewing and/or retrieving materials that are not related to my work in school.
2. Playing computer games or using interactive chat sites, unless the teacher has asked me to do so.
3. Publishing, sharing or giving out personal information about a user (such as home address, e mail address, phone number, etc)
4. Any activity that breaks a school rule.
5. Using another user's password.
6. Use of obscene, racist or offensive language.
7. Insulting or bullying other people
8. Subscribing to any services or ordering any goods.

I know that my teachers can look at the sites I have visited and messages sent or received and if I don't use it properly my Internet privileges will be suspended.

I know that if something inappropriate happens while I'm using the Internet such as someone that I don't know asking me for my name and address I need to tell an adult immediately.

Pupil's Name:___________________________

Pupil's Signature: ___________________________

Appendix 2

ACCESS TO THE INTERNET (PUPILS)

Parents’ Internet Information Letter

Dear Parent/Carer,

Safer Internet Day (S.I.D.) is taking place each year in February to help inform young people of some of the dangers of being online.

I.C.T. including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any I.C.T.

In conjunction with S.I.D. we would encourage you to read and discuss these e-Safety rules (Pupil Agreement) with your child and complete the slip at the bottom of this page as well as the Pupil Agreement overleaf and return it to school promptly. If you have any concerns or would like some explanation please contact the ICT/e-Safety Co ordinator, Mrs Wheeldon or the Principal (028-71302284).

I would also ask you to read the Internet Policy of Drumahoe Primary School and the advice that has been given. You will realise that he/she will be able to access telecommunications networks throughout the world using the Internet. You will understand that this access is designed and intended as an educational tool to enhance learning and teaching and that he/she will receive instruction in the appropriate use of this resource.

Please realise that the internet contains material that is sometimes inappropriate for school purposes and by signing the agreement you support Drumahoe Primary School, in explaining to your child that they are responsible for not intentionally accessing such material. Please acknowledge that unacceptable use of the Internet may result in the temporary suspension or withdrawal of privileges and that you will not hold Drumahoe Primary School accountable for unsuitable materials acquired by him/her through Internet usage at school.

Yours sincerely

T.R. McMaster

T.R. McMaster
Principal

Drumahoe Primary School
Acceptable Use Agreement: Pupils

Parent/Carer signature

We have discussed this and ………………………………………..........(child’s name) agrees to follow the e-Safety rules and to support the safe use of ICT at Drumahoe Primary School.

Parent/CarerSignature…………………………………………………………………

Class ……… Date ………

Appendix 3

P1-3 e-Safety Rules

‘Think then Click’

✓ We only use the internet when an adult is with us.

✓ We only 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 only post polite and friendly messages with an adult’s help.

P4-7 e-Safety Rules

‘Think then Click’

- ✓ We ask permission before using the Internet.
- ✓ We only use websites that an adult has chosen, unless we are asked to do independent research.
- ✓ We tell an adult immediately if we see anything we are uncomfortable with.
- ✓ We ask advice about any webpage, message or pop up that we are not sure about.
- ✓ We only post online with a teacher’s permission after they have approved our post.
- ✓ We make sure posts and messages are polite, respectful and friendly.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don’t know.
- ✓ We do not open links or attachments without permission.
- ✓ We do not attempt to use chat rooms or social networking sites in school.

Appendix 4

Drumahoe Primary School

Acceptable Use Agreement: Staff, Governors & Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of ICT. All members of staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school's UICT/ eSafety Co-ordinator and/or Principal.

- 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 Governing Body.

- I will comply with the ICT system security and **not** disclose any usernames and/or passwords to anyone else **(including other staff members or pupils**) that have been 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 email address, to pupils without the prior permission of the Principal or Governing Body.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that personal data (such as data held on SIMS) 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 Governing Body.

- 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 staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff 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 the Principal. The C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.

- I will respect copyright and intellectual property rights.
- 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 policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will supervise pupils when they are accessing the Internet. I will check websites before allowing pupils to use them to ensure there is no unsuitable content and that material is age appropriate.
- I will not leave any computer 'logged on' with my personal details whereby others may have access to my e-mail account or the internet with 'staff enabled' internet rights.
- I will report deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice immediately to the Principal / ICT Co-ordinator.
- I will make pupils aware of the rules for the safe and effective use of the Internet. These will be displayed in the classroom and discussed with pupils.
- I will adhere to the school's 'Social Networking Policy.'
- I will not use the school systems for commercial transactions unless deemed 'reasonable' by the Principal or Governing Body.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Staff Name: A.N. Other

Signature……..………………………… Date……………………

Full Name………………………………………………………………………………
(Printed)

Position………………………………………………………

Updated – January 2020

Appendix 5

Follow these SMART tips to stay safe online:

SAFE

Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

MEET

Do not meet with someone you have met online. Meeting someone you have only been in touch with online can be dangerous. Remember online friends are still strangers even if you have been talking to them for a long time.

ACCEPTING

Accepting emails, messages, or opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages!

RELIABLE

Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family

TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

Rules for Using Computers/iPads

- ✓ On the C2k network we only use our own login usernames and passwords.
- ✓ We do not access other people's files without their permission.
- ✓ We do not change or delete other people's work.
- ✓ We use the internet for research and school purposes only.
- ✓ We ask permission before entering any website, unless my teacher has already approved that site or has asked me to do independent research.
- ✓ We only post online with a teacher's permission and approval of what we post.
- ✓ We only post messages or content that is polite and responsible.
- ✓ We do not use inappropriate language or find, send or copy offensive messages or pictures.
- ✓ We do not give out names, addresses, phone numbers or any other personal information.
- ✓ We do not open anything that we are unsure about.
- ✓ If we see anything that we do not like or that is inappropriate we tell an adult immediately
- ✓ We do not ignore pop up boxes that we do not understand.
- ✓ We are not allowed to enter chat rooms or social networking sites in school.
- ✓ We understand that school may check our computer files/work and may monitor the websites that I visit
- ✓ We do not bring in memory sticks or digital/electronic devices unless we have been given permission by a teacher.
- ✓ We do not deliberately waste resources such as printer ink or paper.
- ✓ We treat all equipment with respect and will not deliberately damage it.
- ✓ We understand that breaking any of these rules may result in us not being allowed to use the internet, computers or iPads.