Dromore Road Primary School

ONLINE SAFETY POLICY
2025

CONTENTS

1. Key Contacts

Online safety issues may be a safeguarding concern and should be referred to staff with safeguarding responsibility as shown below. This policy should be read in conjunction with other school policies including those for Child Protection, Behaviour, ICT, Mobile Phone, Safe Use of Photos and Videos, Pastoral Care, Remote Learning and Anti-bullying.

All staff should read this policy in full and refer to it when there is any online safeguarding concern for a child or vulnerable adult.

Policy revision summary	
Current Policy Updated	April 2025
Next review due	April 2026

Names of staff with Safeguarding responsibility	
Role	Name
Principal	Mrs McGrath
Designated Teacher	Mrs English
Deputy Designated Teacher	Mrs K. Graham
Deputy Designated Teacher	Mrs O. Graham
Governor with Safeguarding responsibility	Mrs Berry

Policy approval		
Role	Name and contact details	Signature and Date
Chairperson	Mrs E. Cavan	
Principal	Mrs S. McGrath	
Designated Teacher	Mrs L. English	
ICT Coordinator	Mrs L. English	

1.2 Introduction

At Dromore Road Primary School we recognise that the online world provides everyone with many positive opportunities; however, it can also present risks in respect of harm arising out of conduct, content, contact, and commercialisation. We understand that we have a duty of care to ensure that all children and young people are kept safe online and promote their

digital resilience. We aim to teach children 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 role of the Designated Teacher for Child Protection at Dromore Road Primary School is undertaken by Mrs English. This includes acting as a point of contact for online safety.

1.3 Policy Statement

We are committed to providing a secure and safe environment. Everyone regardless of age, ethnicity, religion, gender, gender identity, sexual orientation or any form of disability has the right to equal protection from all types of online harm or abuse.

1.4 Aims and Objectives

The purpose of this policy is to outline the safeguarding measures in place to keep children and staff safe and to prevent harm from occurring when participating in online activities at Dromore Road Primary School.

1.5 Monitoring and Review

This policy, supported by the School's Acceptable Use Agreement (Appendix 2-4) is to protect the interests and safety of the school community. It has been agreed by the staff and approved by the Board of Governors. The policy and its implementation will be reviewed every year, or sooner if deemed necessary due to significant changes in legislation or government guidance on online safety, or because of any other significant event or safeguarding incident.

2. ONLINE HARM AND REPORTING

Online harms are user-generated content or behaviour that is illegal or could cause significant physical or psychological harm to a person. Online harms can be illegal, or they can be harmful to a child or young people, but still be legal. It is essential that children are safeguarded from potentially harmful and inappropriate online material.

Examples of online harms include:

- Online child sexual exploitation or grooming
- Viewing harmful content
- Sharing nudes
- Online bullying
- Online gambling

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** Being subjected to harmful online interaction with other users; for example: peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct:** Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images, and online bullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing, and/or financial scams.

2.1 Online Child Sexual Abuse and Child Sexual Abuse Material

Sexual abuse can happen online as well as offline and includes:

- Showing pornography
- Exposing a child to sexual acts
- Forcing a child to make, view, or share child abuse images or videos
- Making, viewing, or distributing child abuse images or videos
- Forcing a child to take part in sexual activities or conversations online
- Blackmailing a child to share their images unless they pay out money

Online child sexual exploitation occurs when a child is sexually exploited online. They may be persuaded or forced to create sexually explicit photos or videos or have sexual conversations.

Child sexual abuse material is a result of children being groomed, coerced, and exploited by their abusers, and is a form of child sexual abuse. AI can create disturbingly realistic abuse images by manipulating real photos or generating entirely new content. This makes it harder for law enforcement to identify victims and take action against perpetrators

2.2 Sharing Nudes

Sharing nudes or semi-nudes is a term used to describe when persons under 18 send or post nude or semi-nude images, videos, or livestreams online.

It is illegal to take, possess, or share nude images of anyone under 18 and it is important that young people are aware of this. Staff should be alert to their legal obligations including reporting of offences - Section 5 of the Criminal Law Act (NI) 1967 makes it an offence to fail to report a relevant offence. This includes children sharing nudes and semi-nudes.

Police Service of Northern Ireland advice is that if you receive what you believe to be an indecent image, do not delete it and contact the PSNI (Telephone 101 or

https://www.psni.police.uk/report) as soon as you can. You must not send this image to another person or show it to anyone else as you may be committing an offence.

2.3. Report Remove

Young people under 18 who are worried that a sexual image or video of them may have been shared online can use Childline and IWF's Report Remove tool to try to remove it.

Report Remove is a tool that allows young people to report an image or video shared online, to see if it's possible to get it taken down. Provided by Childline and IWF, it keeps the young person informed at each stage of their report and provides further support where necessary. Report Remove can be accessed by visiting childline.org.uk/remove.

A link to this tool is also available in the parent section of the school website.

2.4 Online Grooming

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation, or trafficking. Children and vulnerable adults can be groomed online or face-to-face, by a stranger or by someone they know, for example, a family member, friend, or professional. Groomers may be male or female of any age. Predators can use AI to analyse a child's online activities and tailor their approaches to exploit vulnerabilities more effectively. This can involve creating fake personas that align with the child's interests or emotional states. Some of the signs that a child may be a victim of online grooming can include:

- Being secretive about how they're spending their time, including when online.
- Having an older boyfriend or girlfriend.
- Having money or new things that they can't or won't explain.
- Underage drinking or drug taking.
- Spending more or less time online or on their devices.

- Being upset, withdrawn, or distressed.
- Sexualised behaviour or language.
- Spending more time away from home or going missing for periods of time

Grooming is a criminal offence and occurs where an adult communicates with a person with a view to grooming a child (The Sexual Offences (Northern Ireland) Order 2008). Any concerns about a child should be communicated to the Designated Safeguarding Teacher in line with the school Child Protection Policy.

2.5 Online Blackmail

Online blackmail is when someone threatens to share private information, images, or videos of a person online unless something is done for them.

2.6 Harmful content

As children start to explore the internet, they may come across content that isn't suitable for their age, or that may upset or worry them.

Harmful content can include:

- Sexual content, including pornography
- Violent content
- Fake news
- Hate speech

Content may be legal but could be harmful to a child. Harmful content can depend on a child's age, development, maturity, and support.

2.7 Self Harm

Many online forums, social media, messaging apps, and websites can reinforce or encourage self-harming or suicidal behaviour. Content includes information, pictures, or videos on how to self-harm and describe ways in which children and young people can take their own lives.

Any concerns about a child or young person should be communicated to the Designated Teacher.

2.8 Online Bullying

Online bullying, often referred to as cyberbullying, can occur on any type of device connected to the internet, including social networks, gaming, and websites.

Some examples:

- Abusive or threatening messages or emails
- Abusive comments on social media
- Sharing humiliating videos or pictures of someone
- Spreading rumours online
- Trolling – the sending of menacing or upsetting messages on social networks, chat rooms, or online games
- Excluding children from online games, activities, or friendship groups
- AI-generated deepfakes can be used to humiliate or blackmail children. Predators can create fake explicit content to threaten or coerce children into complying with their demands.

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. texts, social – networking sites or emails. If it takes place within school, cyberbullying will be dealt with in line with the school's overall anti-bullying policy, positive behaviour policy and pastoral services.

In our school children will be taught:

- If they feel they are being bullied by email, through social- networking sites, text or online they should always tell someone they trust.
- Not to reply to bullying, threatening text messages or emails as this could make things worse.
- Not to send or forward abusive texts or emails or images to anyone.

- Keep abusive messages as evidence.
- Not to photograph, film or record anyone without a teacher's permission.

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place outside of school. Should instances of online bullying and abuse be reported to the school by concerned parents, we will advise on how to report the incident to the appropriate authorities. Whilst it is the parent's ultimate responsibility for keeping their child safe at home, the school will also deal with incidences in line with our Anti-bullying policy, if appropriate.

We will keep records of cyber-bullying incidents, if they have occurred within school, to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions.

2.9 Online Gaming

Online games can be a great way for children and young people to keep busy and stay in touch with friends and family, but it is important that they play safely.

Gaming can be a positive pastime providing a way for children to relax, socialise, learn new skills, be part of a team. However, it also carries risks including:

- Grooming by online predators
- Online bullying
- Violent content e.g. extreme violence, warfare, and criminal activity
- Showing explicit sexual acts
- Use of racist, homophobic, or sexist language, or swearing
- Depicting certain groups such as women in a derogatory way
- Gambling

3 ROLES AND RESPONSIBILITIES

3.1 Governors

- To approve and review the effectiveness of the Online Safety Policy.
- To ensure the Designated Teacher with lead responsibility for Safeguarding and Child Protection, including online safety, has the appropriate time, training and support to fulfil the role effectively.
- To support the school in encouraging parents and the wider community to become involved in online safety activities and events.
- To ensure a GDPR compliant framework for storing data and helping to ensure that child protection is always at the forefront and data protection processes support careful and legal sharing of information.
- Ensure that all staff undertake safeguarding and child protection training, including online safety, at induction which is regularly updated.
- Ensure that appropriate filters and monitoring systems are in place.
- Ensure students are taught how to keep themselves safe, including online, as part of providing a broad and balanced curriculum with clear procedures on the use of mobile technology.
- Ensure that the school follows all current online safety advise to keep both students and staff safe.

3.2 Principal

The Principal has overall responsibility for online safety provision, and responsibilities include:

- Ensuring the online safety of members of the school community and fostering a culture of safeguarding, with day-to-day responsibility for online safety delegated to the Designated Teacher.

- Oversee the activities of the Designated Teacher and ensure that their responsibilities in relation to online safety, listed below, are followed, and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and make all staff aware of procedures to be followed.
- Liaise with the designated teacher on all Online Safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Be responsible for ensuring that all staff receive suitable training to carry out their role in safeguarding children online.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of students for online safety issues.
- Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.

3.3 Designated Teacher

- Take lead responsibility for safeguarding and child protection (including online safety) with day-to-day responsibility for online safety issues.
- Be aware of the potential for serious child protection concerns that can arise through online harms.
- Recognise additional risks that pupils with Special Educational Needs or Disabilities (SEND) face online.
- Ensure an effective approach to online safety is in place that empowers the school to protect and educate the whole school community in their use of technology, and establish mechanisms to identify, intervene, and escalate any incident where appropriate.
- Promote an awareness of online safety throughout the school community.
- Keep up to date with the latest trends and issues in online safety and review the online safety policy accordingly.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident and that these are logged in the same way as any other child protection incident.

3.4 Staff

- All staff will be involved in discussions regarding Online Safety and will have access to a copy of the Online Safety policy.
- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.
- Staff are encouraged to sign up to and use the SaferSchoolsNI App and related resources.
- To ensure they have an awareness of current online safety trends and threats.
- Understand that online safety is a core part of safeguarding.
- Read, understand, and sign the staff acceptable use agreement.
- Immediately report any suspected misuse of technology or online safeguarding concern to the Designated Teacher in line with the school safeguarding procedures.
- To ensure Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure that students understand and follow the Online Safety Policy and acceptable use agreements.
- Supervise and monitor the use of digital technologies e.g. iPads in lessons and other school activities and follow policies regarding those devices.
- In lessons where internet use is pre-planned, learners should be guided to sites checked as suitable for their use, and processes are followed dealing with any unsuitable material that is found in internet searches.
- Have a zero-tolerance approach to incidents of online bullying, sexual harassment, discrimination, hatred, etc.
- Model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- A laptop 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.
- Staff are advised not to use their own personal phones or devices for contacting pupils and their families within or outside of the setting in a professional capacity. Staff will have the use of a school phone or device where contact with pupils or parents is required.

- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

3.5 Parents and Carers

Parents and carers have an important role to play in promoting E-Safety. We encourage all parents and carers to become involved in Online Safety discussions with their child. The school website contains links to sites such as CEOP's www.thinkuknow.co.uk which parents can use with their children. It is the responsibility of parents and carers to be fully aware of what their child is doing online. Parents are encouraged to download and use the SaferSchoolsNI App.

Parents and carers should:

- Read and promote the student acceptable use agreement and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's and others' use of technology.
- Parents/ Carers are asked to make a decision as to whether they consent to images of their children being taken/ used in the school, including on our school website.
- Promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology, including on social media.
- Responsible behaviour includes not sharing images or personal details without permission and refraining from posting negative, threatening, or violent comments about others, including the school staff, volunteers, governors, contractors, students, or other parents and carers.

Parents should remember that it is important to promote Online Safety in the home and to monitor Internet use. For example:

- 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 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 (Appendix 1).
- Discuss the fact that there are websites/social networking activities which are unsuitable and age restricted.
- 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. 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.

3.6 Pupils

- Read, understand, sign, and adhere to the Pupil Acceptable Use Agreement.
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school.
- Understand the benefits, opportunities, risks, and dangers of the online world and know who to talk to at school or outside school if there are problems.

4 POLICY DECISIONS

4.1 Teaching and Learning

- The school will plan and provide opportunities within a range of curriculum areas for children to develop their Online Safety skills. Teachers may use CCEA Digital for Life and Work resources, which give pupils opportunities to develop their knowledge and understanding of Online Safety and acceptable online behaviour.
- Online Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught throughout the year as well as specific events such as Safer Internet Day and whole school assemblies.
- Educating pupils on the dangers of technologies that may be encountered outside school is done as part of the Online Safety curriculum and informally when opportunities arise.
- Pupils are where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. 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.
- 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. (Appendix 1)
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be informed that network and Internet use will be monitored.
- 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.

- 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.

4.2 E-mail:

- Children are not currently 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.

4.3 Social Networking:

- The school C2k system will block access to social networking sites for pupils.
- **Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.** However, we accept 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.
- School staff will not add children as 'friends' if they use these sites.
- The school does not support and disapproves of the upload of incidental photographs of pupils taken at school events and would actively seek the support of parents / guardians in implementing this.

4.4 Portable 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. The exception to this may be where devices are connected to speaker systems to play music e.g. during assembly.
- Pupils are not allowed to bring iPads, tablets, iPods, Dictaphones, smart watches or any other device that can photograph, film or record into school. Please refer to our Mobile Phone Policy which should be read in conjunction with this policy.

4.5 iPads:

iPads are used for digital storytelling, internet research and to support teaching and learning across the curriculum via the use of a range of appropriate apps. When using iPads, children will be reminded to be Internet wise and apply their Internet Safety rules. They will not be allowed to use iPads to:

- Take photographs of pupils/staff without permission or direction from the teacher.
- Take videos of pupils/staff without permission or direction from the teacher.

4.6 Managing Video-conferencing:

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

4.7 Publishing Pupil's Images and Work

- Parents/carers must give permission in writing if they wish images of their children to be taken and used on the school website, outside agencies or to be displayed in school. This permission is issued at the beginning of the school year and is considered valid for that school year 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.

- Pupil's work and photographs will only be published by outside agencies with the permission of the pupil and parents.

4.8 Remote Learning

At Dromore Road Primary School the Seesaw App is used as a digital communication app between school and home. Please refer to our Remote Learning Policy which should be read in conjunction with this policy.

4.9 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 Online Safety rules. These Online Safety rules will also be displayed clearly in all rooms and in the school corridor.
- 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 Online Safety rules and within the constraints detailed in the school's Online 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.

4.10 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.
- 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.

4.12 Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by the Senior Leadership Team.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the Online Safety incident logbook.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Complaints regarding online bullying will be dealt with in line with the school Anti-Bullying Policy.
- As part of the Acceptable use agreement children will know that if they deliberately break rules they could be stopped from using the internet and that parents/carers will be informed.

APPENDIX 1
Safety Rules for Children

Follow These SMART TIPS

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 Proctection Committees

APPENDIX 2

DROMORE ROAD PRIMARY SCHOOOL

An Acceptable Use of the Internet

For Pupils in Primary 1-3

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- I will only use my own login username and password.
- I will not change or delete other people's work.
- I will only use websites that my teacher has approved.
- If I see anything I am unhappy with I will tell a teacher immediately.
- I will not bring in memory sticks, mobile devices and recording devices (e.g. iPad, tablet, iPod, smart watches) to school unless I have been given permission by my teacher.
- I will never photograph, film or record anyone unless I have been given permission from my teacher.
- I understand that the school may check my saved work.
- I will treat all ICT equipment with care.
- **I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/carers will be informed.**

APPENDIX 3

DROMORE ROAD PRIMARY SCHOOOL

An Acceptable Use of the Internet

For Pupils in Primary 4-7

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- On the network, 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 before entering any website, unless my teacher has already approved that site.
- I will use the Internet for research and school purposes only.
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks, mobile devices and recording devices (e.g. iPad, tablet, iPod, smart watches) to school unless I have been given permission by my teacher.
- I will never photograph, film or record anyone unless I have been given permission from my teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I will treat all ICT equipment with care
- I will always treat others online as I would like to be treated.

DROMORE ROAD PRIMARY SCHOOL

Acceptable Use Agreement
For Pupils

Please complete and return this form to your child's class teacher

Pupil's Name		**Class Teacher**	
I have discussed and understood the Online Safetyagreement and will follow the rules which are there to keep me and the school safe.			
Pupil Name (print)			
Pupil Signature		**Date**	

Parents Name	
As the parent or legal guardian of the pupil above, I have read and discussed the Online Safety agreement with my child and give permission for my child to access the internet at school. I will encourage them to abide by these rules. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety. I will ensure that any photographs taken during school events that include other children will not be shared using social media.	

Parents Name (print)			
Parents Signature		**Date**	

DROMORE ROAD PRIMARY SCHOOL

Acceptable Use 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.

- 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

Name		
Date		**Signed**