



Online Safety and Acceptable Use of the Internet and Digital Technologies Policy

Date	Policy Reviewed	Policy Amended	Added to Website

Section 1- Introduction

- 1.1 Vision
- 1.2 Vision for Information & Communication Technology
- 1.3 Introduction
- 1.4 Rationale for policy
- 1.5 Scope of policy

Section 2- Roles and Responsibilities

- 2.1 ICT Co-ordinator
- 2.2 Head of Pastoral Care/Designated Teachers for Child Protection
- 2.3 Principal and Board of Governors
- 2.4 All school staff

Section 3- Risk Assessment

- 3.1 Content risks
- 3.2 Contact risks
- 3.3 Commercial risks
- 3.4 Conduct risks

Section 4- Code of Safe Practice

- 4.1 Code of Practice for pupils
- 4.2 Code of Practice for staff
- 4.3 Sanctions

Section 5- Online Safety

- 5.1 Internet safety awareness for pupils
- 5.2 Internet safety awareness for staff
- 5.3 Internet safety awareness for parents/guardians
- 5.4 Teaching and support staff password security
- 5.5 Pupils password security
- 5.6 Health and Safety
- 5.7 Digital and video images of pupils
- 5.8 School website
- 5.9 Storage of images
- 5.10 Mobile phones
- 5.11 Social software

Section 6- Data Protection and Filtering

- 6.1 The EU General Data Protection Regulation & the Data Protection Act
- 6.2 Filtering
- 6.3 Breaches of filtering systems

Section 7- Policy Review

Appendices

- Appendix 1 Bring Your Own Device User Agreement for Staff
- Appendix 2 Pupils Acceptable Use Agreement
- Appendix 3 Staff Acceptable Use Agreement
- Appendix 4 Online Safety and Acceptable Use Incident Log
- Appendix 5 SMART tips

Seagoe Primary School

Online Safety and Acceptable Use of the Internet and Digital Technologies Policy

Section 1- Introduction

1.1 Vision

At Seagoe Primary School we are proud to be an inclusive school providing high quality, creative and challenging education within a secure, caring, and happy environment, where every child experiences a sense of enjoyment and achieves their full potential. We aim to provide each child with a broad and balanced education which encompasses the requirements of the Northern Ireland Curriculum (CCEA, 2007) and the social, moral, physical, and aesthetic aspects befitting the needs of adult life. Emphasis is placed on each pupil developing a caring and respectful attitude towards peers, adults, the community, and themselves. Ultimately, we seek to fulfil the vision of preparing pupils as best we can for adult life.

1.2 Vision for Information & Communication Technology

At Seagoe Primary School, we believe that digital technologies are very powerful resources which can enhance and transform teaching and learning. Given the school's vision of preparing pupils for life, we are committed to promoting pupils' skills within the use of technology across the curriculum. We believe that technology has an integral role to play in helping pupils to achieve their full potential, assisting them in overcoming barrier to learning and in supporting learning throughout the school community. Ultimately, our vision is to encourage and nurture within our pupils, and the entire school community, knowledge, skills, and qualities that will make them responsible digital citizens now and in the future. We aspire to safely and confidently equip pupils to face the exciting, new, and ever developing opportunities and challenges presented by constantly evolving technology.

1.3 Introduction

In Seagoe Primary School we believe that the internet and other digital technologies are very powerful resources which can enhance and potentially transform learning and teaching when used effectively and appropriately. The internet is an essential element of 21st century life for education, business, and social interaction. Our school provides pupils with opportunities to use the excellent resources on the internet, along with developing the skills necessary to access, analyse and evaluate them in a safe, responsible manner.

The Department of Education in Northern Ireland (DENI) recognises the important role digital technologies have in modern day life noting:

'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' (Circular, 2007, p.1)

The Department of Education refers to the Safeguarding Board for Northern Ireland's 2014 report on e-safety, stating that *'young people's extensive use of technology leaves no doubt over the importance of online safety'* (Circular, 2016, p. 27).

As such, given the school's vision of preparing pupils for life, this document sets out the policy and practices for safe and effective use of the internet in Seagoe Primary School. This policy has been drawn up by the ICT Co-ordinator under the leadership of the Principal, with valuable input from the staff. It has been approved by Governors and is made available to all parents through contacting the School Office. The policy and its implementation will be reviewed annually.

1.4 Rationale for Online Safety Policy

'All schools should have their own e-safety policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. E-safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills' (Circular, 2013, p.25).

It is the responsibility of the school, staff, governors, and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people can use the internet and related digital technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Online safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The school must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents/guardians) be responsible users and stay safe while using the internet and other communication technologies for educational, personal, and recreational use.

1.5 Scope of Policy

This policy applies to all members of the school community who have access to and are users of the school ICT systems, both in and out of the school. In relation to incidents that occur during school hours, we will work with parents, staff, and pupils to ensure the online safety of all involved, apply sanctions as appropriate and review procedures.

In relation to online safety incidents that occur outside of school hours, the school will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. Online safety outside school hours is primarily the responsibility of parents/guardians. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the school community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Incidents of cyber-bullying will be dealt with through the school's Anti-Bullying Policy. Any issues that arise inside school, because of online safety incidents outside of the school, will be dealt with in accordance with school policies. This policy works alongside and incorporates other school policies, such as the Safeguarding and Child Protection Policy and the Anti-Bullying Policy.

Section 2- Roles and Responsibilities

Recognising the importance of online safety, and its interdependence on other school policies and aspects of school life, the Board of Governors have appointed several key staff to monitor the implementation and review of this policy. All staff however should recognise the important role they play in implementing this policy.

Designated Governor for Online Safety	Mr A Woods
Principal	Mrs C Poots
ICT Co-ordinator/Deputy Designated Teacher for Child Protection	Miss J Connolly
Head of Pastoral Care/Designated Teacher for Child Protection	Mrs J Curlett

2.1 ICT Co-ordinator

The ICT Co-ordinator will lead online safety, takes day-to-day responsibility for online safety issues, and has a leading role in establishing and reviewing the school's policies/documents relating to online safety and acceptable use.

The ICT Co-ordinator will:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide training and advice to staff as appropriate.
- Liaise with C2k, iMex and other external agencies.
- Liaise with the EA and DENI on online safety developments as appropriate.
- Receive reports of online safety incidents and create a log of incidents to inform future practice.
- Form a member of the Child Protection and Safeguarding Team.
- Meet regularly with the Head of Pastoral Care to monitor and review Incident Log.
- Meet regularly with the Designated Teacher for Child Protection to investigate abuse of social network sites by pupils.
- Attend relevant meetings with Board of Governors as appropriate.

- Discuss current issues with the Senior Leadership Team and review incident logs.
- Monitor and report to Senior Staff any risks to staff of which the co-ordinator is aware.
- Monitor the curricular opportunities for implementation of online safety as part of the ICT curriculum.
- Consult with parents and outside agencies as appropriate in relation to online safety education.
- Ensure pupils and staff comply with the Acceptable Use Agreements (Appendices 2 and 3) and BYOD Policy (Appendix 1).
- Reconcile all returns of agreements appropriately.

2.2 The Head of Pastoral Care/Designated Teachers for Child Protection

The Designated Teacher for Child Protection (and their deputy) will be trained in online safety issues as appropriate and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

In addition, the Designated Teacher for Child Protection, as the Head of Pastoral Care within the school, will meet regularly with the ICT Co-ordinator to monitor and review the Incident Log.

2.3 The Principal and Board of Governors

The Principal has a duty of care for ensure the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the designated members of staff. The Principal is responsible for appointing members of staff to act as C2K Managers, and for authorising a Register of Access to the school's confidential files and programmes.

The Principal and ICT Co-ordinator will be kept informed about online safety incidents.

The Principal will deal with any serious online safety allegations being made against a member of staff.

The Principal and Senior Leadership Team are responsible for ensuring that the ICT Co-ordinator and other relevant staff receive suitable training and allocated time to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Board of Governors is responsible for the approval of the Online Safety and Acceptable Use of the Internet and Digital Technologies Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports from the Principal. Recognising the importance of online safety and given the fact that many of the issues which may arise will be of a safeguarding or child protection nature, the Board of Governors have decided to appoint the Designated Governor for Safeguarding and Child Protection as the Designated Governor for Online Safety. The Designated Governor for Online Safety will regularly review online safety logs as appropriate.

2.4 All School Staff

As well as having key members of staff appointed to review and implement this policy, it is important that all staff realise and understand that they have the responsibility to ensure that:

- They have an up-to-date awareness of online safety matters and follow the current Online Safety and Acceptable Use of the Internet and Digital Technologies Policy.
- They have read, understood, and signed the school's Staff Code of Practice Acceptable Use Policy.
- They report any suspected misuse or problem to the ICT Co-ordinator or Head of Pastoral Care.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- That pupils have a good understanding of research skills and the need to avoid plagiarisms and uphold copyright laws.
- They monitor ICT activity in lessons and extra-curricular activities.

- They are aware of online 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 regarding these devices.
- Undertake all online safety training as organised by the school.
- Pupils understand the Pupil Code of Practice Acceptable Use Agreement.

Section 3- Risk Assessment

'21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity, they need to learn to recognise and avoid these risks- to become "Internet- wise" and ultimately good "digital citizens". Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy' (DENI E-Safety Guidance, Circular, 2013, p.25).

The main areas of risk for the school can be categorised as the content, contract, commercial and conduct of activity.

3.1 Content risks

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

Children need to 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.

3.2 Contact Risks

Children may come into contact with someone online who may wish to harm them. Some adults use chat rooms, online gaming, social media, or email to communicate with children for inappropriate reasons.

Children need to be taught:

- That people are not always who they say they are.
- That technology such as voice changing software is available online.
- 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 anyone contacted via the Internet without a responsible adult.

3.3 Commercial Risks

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

Children need to 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.
- Not to believe everything they see online to be true.
- Be aware of scam emails, how to filter these and be wary of links within these.

3.4 Conduct Risks

Children need to appreciate that bullying, entrapment, and blackmail can take place online as well as in person. When connecting with peers and others online, pupils may be in a position where they receive harmful or hurtful statements or threats. Pupils themselves may be involved in issuing such comments or threats.

Children need to be taught that:

- To report any such instances to a teacher within school, or to an appropriate adult.
- To seek assistance or help if they feel they are victims of bullying, entrapment, or blackmail.
- To understand that their online behaviour is equally as important as that in their real lives and consequences exist for their actions online in their everyday lives.
- Not to send appropriate images of themselves or others.
- Understand that once published, materials leave a digital footprint online, and will always be traceable or accessible.

If children use the internet in places other than at school, they need to be educated about how to behave online and to discuss problems. They need to be educated as to how to report issues online, such as the instant reporting system provided by CEOP. As with all other risks, it is impossible to eliminate these 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. There are no totally effective solutions to the problems of internet safety. Consequently, teachers, pupils and parents must be vigilant.

Many of the risks reflect situations in the offline world and it is essential that this Online Safety and Acceptable Use of the Internet and Digital Technologies Policy is used in conjunction with other school policies, including Behaviour, Children Protection and Safeguarding and Anti-Bullying.

Section 4- Code of Safe Practice

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. The Code of Safe Practice (Acceptable Use Policies) for Seagoe Primary School makes explicit to all users (staff and pupils) what is safe and acceptable and what is not.

The scope of the code covers fixed and mobile internet, school PCs, iPads, laptops, and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils have brought onto school premises (such as mobile phones, camera phones, private iPads, Apple Watches, private laptops, and tablets) are subject to the same requirements as technology provided the school. Any personally owned equipment being used on school premises must comply with the Bring Your Own Device (BYOD) policy (Appendix 1).

The ICT co-ordinator will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

4.1 Code of Practice (Acceptable Use Policy) for Pupils

Pupils access to the internet is through a filtered service provide by C2K, and the Classnet filtered service for iPads (as risk assessed by the Board of Governors), which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents annually before pupils access the internet.

For pupils in Key Stage 1 and 2, they sign the Code of Practice Acceptable Use Agreements and copies of these are held on file by the class teacher (Appendix 2). Pupils in Foundation Stage are closely monitored during their use of ICT equipment and are taught to care for equipment and what to do if they see or hear something that upsets them. In addition, the following key measures have been adopted by Seagoe Primary School to ensure our pupils do not access any inappropriate material:

- The school's Code of Practice for use of the internet and other digital technologies is made explicit to all pupils and is displayed prominently in suitable locations, such as the ICT area.
- Our Code of Practice is reviewed each school year and signed by pupils/parents.
- Pupils using the internet will normally be working in highly- visible areas of the school.

- All online activity is for appropriate educational purposes and is supervised, where possible.
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group. Where the task involved pupils locating suitable websites themselves, explicit instruction will be provided by teachers of how best to locate appropriate sites, and how to evaluate their authenticity and appropriateness.
- Pupils in all Key Stages are educated in the safe and effective use of the Internet, through a number of selected programmes.

It should be accepted that however rigorous these measures may be, they can never be 100% effective. Neither the school, nor C2K or Classnet, can accept liability under such circumstances.

4.2 Code of Practice (Acceptable Use Policy) for Staff

Staff are aware of the important role they play in promoting and protecting pupils' safe use of digital technologies. Each year members of staff using the school's ICT system sign and agree to the Acceptable Use Agreement for Staff (Appendix 3). Staff have also agreed that:

- Pupils accessing the internet should always be supervised by an adult.
- All pupils are aware of the rules for safe and effective use of the internet. These are displayed in prominent locations within the school and discussed with pupils.
- All pupils using the internet have written permission from their parents.
- Recommended websites for each year group have been approved by class teachers. Any additional websites used by pupils should be checked beforehand by teachers, to ensure, as far as possible, 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.
- In the interests of system security, staff passwords should not be shared.
- Teachers are aware that the C2K My School system tracks all internet use and records the sites visited. The system also logs emails and messages sent and received by individual users. It is important that users are aware that a request may be made by the Principal to access such tracking information, and by signing the Acceptable Use Policy for Staff, members of staff authorise such information to be released to the Principal/Board of Governors.
- Teachers 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.
- Staff understand that any work carried out on the C2k system whilst in the employment of Seagoe Primary School remains the property of the school.
- Photographs of pupils should, where possible, be taken with a school camera/iPad and images stored on a centralised area on the school network, accessible to staff only.
- School systems may not be used for unauthorised commercial transactions.

4.3 Sanctions

Incidents of technology misuse which arise will be dealt with in accordance to the school's discipline policy. Minor incidents will be dealt with by the ICT Co-ordinator and Head of Pastoral Care, in consultation with the Principal, and may result in a temporary or permanent ban on internet use. Such incidents may be reported by staff or pupils.

In the first instance, for minor breaches of the Acceptable Use Policy for pupils, a reminder of the Acceptable Use Policy will be given. This will be logged in the Incident Log (Appendix 4) and saved appropriately. On a second breach, and for more serious incidents as identified by the ICT Co-ordinator/Head of Pastoral Care, the incident will be recorded in detail within the school's Online Safety and Acceptable Use Incident Log and saved appropriately. Incidents involving child protection issues will be dealt with in accordance with school safeguarding and child protection procedures. Where incidents of technology misuse involve members of staff, and it is deemed warranted by the Principal, they will be dealt with by the Board of Governors through the normal disciplinary measures. Within all circumstance, where a potential breach of online safety has occurred, it will be registered in the school's Incident Log or Online Safety and Acceptable Use Incident Log (Appendix 4).

Section 5- Online Safety

In Seagoe Primary School we believe that, alongside having a written safety policy and acceptable use agreements, 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 as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

5.1 Internet Safety Awareness for pupils

Rules for the acceptable use of the internet are discussed with all pupils and are prominently displayed in key areas in the school. The school has in place a preventative and progressive online safety curriculum from Foundation Stage to Key Stage Two. This scheme ensures that online safety forms the main focus of at least two lessons each half term. The scheme is organised on the eight themes identified by the United Kingdom Council for Child Internet Safety. These themes are as follows:

1. Managing online information
2. Privacy and safety
3. Copyright and ownership
4. Health, wellbeing, and lifestyle
5. Self-image and identity
6. Online relationships
7. Online reputation
8. Online bullying

In addition, online safety is incorporated into planning for ICT across the curriculum, including Internet Safety Awareness using a range of online resources e.g. CEOP, Think You Know programmes and taking part in Internet Safety Day and other appropriate events throughout the year.

5.3 Internet Safety Awareness for Parents/Guardians

The Acceptable Use Policy and Online Safety Policy are available for parents/guardians by request. The Acceptable Use Policy for pupils is sent home at the start of each school year for parental signature. Online safety leaflets for parents and guardians are also sent home as appropriate.

Points for parents/guardians to consider

It is important to promote Internet Safety in the home and to monitor internet use. Keep the computer in a communal area of the home.

- Ask children how the computer works.
- Monitor online 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 5).
- Discuss the fact that there are websites which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information on the internet.
- 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.
- Be aware of the vast array of apps available to pupils on their mobile phones and other mobile technical devices, with particular attention to the minimum age for use of such software.
- Check parental control settings on devices which connect to the internet.
- Consider keeping your WIFI password private from children, so they cannot share it with their friends when they visit your house. Remember that any activity which visitors to your home undertake whilst using your internet access point is traceable to your address and thus may be deemed your responsibility.

5.4 Teaching and Support Staff: Password Security

Password security is essential for staff, particularly as they can access and use pupil data.

- Staff are expected to have secure passwords which are not shared with anyone.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.
- Staff should ensure iPads are secured appropriately.

5.5 Pupils: Password Security

- All users read and sign a Code of Practice Acceptable Use Agreement to demonstrate that they have understood the school's Acceptable Use Policy.
- Pupils are expected to keep their passwords secret and not to share with others, particularly their friends. In upper Key Stage 2, pupils should be encouraged to select an appropriate secure password of their own.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers, or others.

5.6 Health and Safety

Seagoe Primary School has attempted to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT area. Pupils are always supervised when panel boards, Interactive Whiteboards, Digital Projectors, computers, laptops and iPads are being used.

5.7 Digital and Video Images of Pupils

Parental permission is sought at the start of each school year to cover the use of photographs of pupils on the school website, in the local press and for displays etc. within school and written permission must be obtained from the parent/guardian.

5.8 School website

Our school website promotes and provides up to date information about the school, as well as giving pupils and opportunity to showcase their work and other aspects of school life. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible with general labels/captions, however individual images and names can be used to celebrate individual successes.
- The website does not include home addresses, telephone numbers, personal emails or any other personal information about pupils or staff.
- Website links selected by teachers may be put on the website for pupils to access outside of school- sites will be previewed and checked regularly.

5.9 Storage of images

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network, accessible only to teaching staff.

5.10 Mobile phones

Pupils have no need to use mobile phones whilst in school. Should emergency contact between parents and pupils be required, then the school secretary is available to relay such emergency information. Pupils in upper Key Stage 2 who wish to bring a mobile phone to school do so at their own risk. The school accepts no liability for devices brought into school. Mobile phones are not permitted to be used by pupils on school grounds or on school trips. They should remain turned off and in the pupil's school bag, remaining their responsibility and at their own risk. If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/guardians by the Principal.

5.11 Social software

Chatrooms, blogs, and other social networking sites are blocked by C2K and Classnet filters, so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our internet safety education for pupils.

Instances of cyber-bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's Discipline Policy and child protection procedures. Both parents/guardians and pupils should be aware that messages relating to individual members of staff or the school which are derogatory in nature may be reported to the Police Service of Northern Ireland, who may treat such instances as harassment.

Section 6- GDPR, The Data Protection Act and Filtering

6.1 The EU General Data Protection Regulation and The Data Protection Act

The school complies with the EU GDPR and the Data Protection Act, and staff are regularly reminded of their responsibilities. The Principal is responsible for authorising a Register of Access to the school's data. Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly logged off or locked at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media the following guidance must be followed:

- The device is password protected with appropriate encryption software.
- The device offers approved virus and malware checking software.
- The data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

The school has in place a comprehensive Data Protection Policy and Privacy Notices, which are available from the Principal and school office on request.

6.2 Filtering

All devices on the school network benefit from industry leading filtering protection. Managed devices benefit from filtering managed through C2K. The Classnet system is filtered and managed by To Do Tech.

6.3 Breaches of Filtering System

Pupils are aware that any misuse of mobile phones/websites/email/iPads should be reported to a member of staff immediately.

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the internet and digital technology may give pupils access to undesirable information or images.

Pupils are regularly reminded that should they encounter inappropriate material online; they must immediately leave the website and inform an adult.

Should a pupil or teacher encounter unsuitable material through the managed service, this should be reported immediately to the ICT Co-ordinator, and this will then be reported to C2K. Classnet filtering breaches will be reported to and managed by the service provider. In all circumstances, such breaches will be recorded in the school's Online Safety and Acceptable Use Incident Log, which will be reviewed regularly by the Principal.

Section 7- Policy Review

Digital and internet technology and school use of resources will develop and change with time. It is our intention to revise and update our Online Safety and Acceptable Use Policy annually or as appropriate and where necessary.



Bring Your Own Device (BYOD) User Agreement- Staff Declaration

I request permission to use my own personal ICT device in school.

Device Type/s: _____

I have read and understood the Online Safety and Acceptable Use of Internet and Digital Technologies Policy, and I agree to be bound by all guidelines, rules and regulations contained within it. I agree to use the device for educational use only.

Disclaimer- Please read carefully

The school accepts no liability in respect of any loss/damage to personal ICT devices while at school or during school activities. The decision to bring a personal ICT device into school rests solely with the member of staff, as does the liability for any loss/damage.

I understand the disclaimer and accept that I am personally and solely responsible for the correct care, safety and security of the device. I understand that the school accepts no liability in respect of any personal ICT device used in school by a member of staff.

I understand that I may only connect to the school's filtered WIFI networks once I have signed and returned this BYOD agreement, and agree that I shall not try to circumnavigate or diminish the filtering security of the networks.

I aware that the C2K My School system and the Classnet system tracks all internet use and records the sites visited. The systems also log emails and messages sent and received by individual users and log all activity. It is important that users are aware that a request may be made by the Board of Governors, through the Principal, to access such tracking information, and by signing the Acceptable Use Agreement for Staff, members of staff authorise such information to be released to the Principal/Board of Governors.

This contract will remain force throughout my time at school and it may be revised to take account of technological advancements in the interest of pupil and staff safety. Should I change my device/s, I agree to update this record with the ICT Co-ordinator.

Please complete and return this form to the ICT Co-ordinator.

Name (please print): _____

Signed: _____

Date: _____



Acceptable Use of the Internet and Digital Technology for Pupils

Pupil's Name: _____ **Class:** _____

Children should know that they are responsible for their use of the internet and digital technology in school and that they must use it in a safe and appropriate manner. They must also realise that this agreement extends to the use of any technology or device on school premises, whether personally or school owned. Please discuss these guidelines with your child and stress the importance of the safe use of digital technology, including the Internet.

As a pupil at Seagoe Primary School, I agree that:

- I will take very good care of all equipment I use in school, treating it with respect.
- On the C2k network and any other appropriate apps, 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 accessing 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-mails in school when directed by my teacher using my C2k email account. I will make sure that the messages I send are polite and responsible.
- I understand that I am not allowed to access any private email accounts I may have whilst in school.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail or communicating digitally.
- When sending an 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 in school.
- If I see anything I am unhappy with or receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks or CD-ROMs from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/e-mails and may monitor the internet sites that I visit.
- I understand that I must not use my mobile phone whilst on school premises. If I bring a phone to school, it must remain switched off and in my school bag, and that it remains my responsibility. The school accepts no responsibility for it should it go missing or get damaged.
- I understand that I should not bring wearable technology, such as Apple watches, to school.
- I understand that I am not allowed to bring my own personal devices to school without the prior permission of the Principal/ICT Co-ordinator and that I must not try to connect devices to the school's networks.
- I understand that if I deliberately break these rules, I could be stopped from using the internet/e-mail/digital technologies, my Parent/Guardian will be informed and sanctions will apply.
- I understand that the school computer/iPad system log and monitor my use of the devices.
- I will use Purple Mash safely and appropriately to aid my learning and showcase my achievements across the curriculum.

Parents/Guardians

As noted in the school's Online Safety and Acceptable Use Policy, both parents and staff have an important role to play in educating children on how best to use digital technology safely. As parents, it is important to monitor and protect your child's online activity at home. We all, parents and teachers, should remember that we are important role models in the lives of our children. We must all remember that any digital communication, such as social networks, are still subject to the rule of law. We must work together in partnership to educate our children and keep them safe online. By signing below, you accept the above acceptable use agreement and consent to your child using Purple Mash, noting the terms and conditions.

Signature of Pupil: _____

Signature of Parent/Guardian: _____

Date: _____



Code of Practice Acceptable Use Agreement for Staff

The computer system and associated digital technology 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 Acceptable Use Policy has been drawn up to protect all parties- the pupils, the staff, and the school.

By signing this agreement, you recognise and accept that the Board of Governors reserves the right to examine or delete any files that may be held on its computer system, to monitor any internet sites visited and to monitor and review the use of the school's digital technology.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the ICT Co-ordinator. By signing, members of staff accept and agree that:

- All internet activity and use of digital technology should be appropriate to staff professional activity or the pupils' education.
- Access should only be made via your given authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school's ICT system, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all emails sent and for contacts made that may result in emails being received.
- Use for personal financial gain, gambling, political purposes, or advertising is forbidden
- Posting anonymous messages and forwarding chain letters is forbidden.
- As emails 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 and could be reported to the police.
- Teachers 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.
- Staff understand that any work carried out in the C2K system whilst in the employment of Seagoe Primary School remains the property of the school.
- Photographs of pupils should, where possible, be taken with a school device and images stored on a centralised area on the school network, accessible only to staff.
- School systems may not be used for unauthorised commercial transactions.
- Members of staff agree to maintain the confidentiality of records and information held digitally within the school, ensuring they meet the requirements of the GDPR and the Data Protection Act.
- Staff should not be directly connected on social media to pupils at the school. They should also ensure that their social media does not give cause of the school to be called into disrepute.
- Staff should not use mobile phones in the presence of children within classrooms. During the teaching day, mobile phones should remain out of sight from children, unless authorised by the Principal. Staff should, as far as possible, seek to use their mobile phones in the staffroom or office away from pupils.
- Staff accept that they may not connect personal device to the school's networks, including the Classnet and C2K WIFI networks, without accepting and returning to the ICT Co-ordinator a form of agreement to the school's Bring Your Own Device Policy.

Teachers are aware that the C2K My School and Classnet systems tracks all internet use and records the sites visited. The systems also log emails and messages sent and received by individual users and log all activity. It is important that users are aware that a request may be made by the Board of Governors, through the Principal, to access such tracking information, and by signing the Acceptable Use Agreement for Staff, members of staff authorise such information to be released to the Principal/Board of Governors.

Name (please print): _____

Signed: _____

Date: _____





Online Safety and Acceptable Use Incident Log

Date of incident	
Time of incident	
Pupils or staff involved	
Location of incident	
Device number(s)	
Computer account(s) involved	
Details of incident	
Actions taken and reasons	
Outcome	
How can the school try to better prevent this incident occurring in the future?	
Signature of ICT Co-ordinator	
Signature of Head of Pastoral Care	
Signature of Principal	
Signature of Designated Governor for Online Safety	


BE SMART ONLINE




S SAFE  Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.

M MEET  Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk

A ACCEPTING  Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.

R RELIABLE  You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.

T TELL  Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk

BE SMART WITH A HEART  Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.

