Safer Internet Policy

(Online Safety)

(Curriculum & Pastoral Care)

2019

Ashgrove Primary School

Learning, Caring, Growing Stronger Together

SAFER INTERNET POLICY

A PASTORAL CARE & CURRICULUM POLICY

Agree Date	Review Date	Person Responsible for Review
2019	**2021**	**K. Flaherty**

Context

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circular 2011/22 on Internet Safety.

The above circulars state that:
"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."
This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Ashgrove Primary School.

Rationale

> *"The school's actions on and governance of online safety must be reflected clearly within the school's safeguarding arrangements and Online Safety Policy. Safeguarding and promoting pupils' welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities."*
>
> *DENI Online Safety Guidance, Circular number 2016/27*

It is the responsibility of the schools, staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications 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 in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Care and responsibility

Our mission statement is **'Learning, Caring, Growing Stronger Together'**. As a school we are focused on realising and achieving this potential for every child in our community.

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 will 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 Online Safety Guidance, Circular number 2013/25

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. With these opportunities we also have to recognise the risks associated with the internet and related technologies.
The use of these 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

As with all other risks, it is impossible to eliminate the risk completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any scenarios which may arise.
In Ashgrove Primary School we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach pupils appropriate behaviors 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.

What are the main risks?

The main areas of risk for the School can be categorized as the Content, Contract and Conduct of activity.

1. **Content**
   - Access to illegal, harmful or inappropriate images or other content.
   - Access to unsuitable video / internet games.
   - An inability to evaluate the quality, accuracy and relevance of information on the Internet.

2. **Contact**
   - Inappropriate communication / contact with others, including strangers.
   - The risk of being subject to grooming by those whom they may make contract on the Internet.
   - Cyber-bullying.
   - Unauthorized access to / loss of / sharing of personal information.

3. **Conduct**
   - The potential for excessive use which may impact on the social and emotional development and learning of the young person.
   - Plagiarism and copyright infringement
   - Illegal downloading of music or video files
   - The sharing / distribution of personal images without an individual's consent or knowledge.

Many of these risks reflect situations in the offline world and it is essential that this Online Safety policy is used in conjunction with other School policies e.g. Positive Behavior, Child Protection, Anti-Bullying and Acceptable Use, Mobile devices, Disposal of documents.
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' 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

Scope of the 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 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 the parents. 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. Any issues that arise inside school, as a result of Online Safety incidents outside of the School, will be dealt with in accordance with School Policies.

Roles and Responsibilities

As E-Safety is an important aspect of Child Protection within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator (Mrs Flaherty) to keep abreast of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of E-Safety throughout the school. The Principal/ICT Co-ordinator have the responsibility to update Senior Management and Governors with regard to E-Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

Online Safety Coordinator

The Online Safety Coordinator will lead the Online Safety Committee and takes day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the Schools policies/documents.

The Online Safety Coordinator 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 for staff
- Liaise with C2K and school ICT technical staff
- Liaise with the EA and DENI on Online Safety developments
- Liaise with the technical staff
- Receive reports of Online Safety incidents and create a log of incidents to inform future Online Safety developments
- Meet regularly with Principal to investigate abuse of social network sites by pupils
- attend relevant meetings with Board of Governors
- discuss current issues, review incident logs
- monitors and reports to Principal and senior staff any risks to staff of which the Online Safety coordinator is aware
- oversees the application of the 360 Degree Safe Mark Award.

Online Safety Officers / Designated Child Protection Officer / Designated Deputy Child Protection Officer

The Child Protection Officer (V Luney) and their deputy (K Coulter) will be trained in Online Safety issues 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

Online Safety Committee

The Online Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online Safety and the monitoring of the Online Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governors.

Committee Members:

- Online Safety Coordinator: Mrs. Karen Flaherty
- School Principal: Mr R Smith
- The Child Protection Officer: Mrs. Valerie Luney
- ICT Coordinator : Mrs Karen Flaherty
- E- Safety Staff Representative : Mrs Karen Flaherty
- ICT Teacher Representative - Mr Iain Hutcheson
- Governor – Mr Billy Edwards

Members of the Online Safety Committee will assist the Online Safety Coordinator with:

- The production and review of the school Online Safety policy and related documents.
- mapping and reviewing the Online Safety curricular provision, ensuring relevance, breadth and progression
- monitoring incident logs from the pastoral team
- consulting parents/ carers and the pupils about the Online Safety provision
- monitoring improvement actions identified through use of the 360 Degree Safe Self Review Tool

The Principal and Senior Leadership Team:

The Principal has a duty of care for ensuring 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 Online Safety Officers.

The Principal and Online Safety Officer will be kept informed about Online Safety incidents.

The Principal will deal with any serious Online Safety allegation being made against a member of staff.

The Principal and SLT are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.

Governors:

Governors are responsible for the approval of the Online Safety 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.

Mrs Karen Flaherty reports to the Governors on Online Safety matters.

The designated Online Safety Governor is **Mrs G McDade-Hastings**

She will:

- have regular meetings with the Online Safety Coordinator
- regularly monitor Online Safety incidents logs

Training will be given to the Governors by:

- Attendance at training provided by relevant external agencies / staff in school
- Participation in school's training / information sessions for staff or parents

Network Manager- Iain Hutcheson

The Network Managers will monitor that C2K Online Safety measures, as recommended by DENI, are working efficiently within the school.

- that C2k operates with robust filtering and security software
- that monitoring reports of the use of C2k are available on request
- that the school infrastructure and individual workstations are protected by up-to-date virus software.
- that the school meets required Online Safety technical requirements that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed the filtering policy is applied and that its implementation is not the sole responsibility of any single person that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- that the "administrator" passwords for the school ICT system, used by the Network Managers must also be available to the Principal and kept in a secure place

Teaching and Support Staff

The Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of Online Safety matters and of the current school Online Safety policy and practices.
- They have read, understood and signed the school's Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the Online Safety Coordinator.
- Digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level only carried out using official school systems – either C2K or School Gmail accounts. Emails should be sent in accordance with the School's guidance.
- Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- Staff understand and follow the school Online Safety Policy and Acceptable Use Policy.

- That students have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act 1998)
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of Online Safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- Undertake all Online Safety training as organized by the school

E-Safety Skills Development for Staff

• All staff will receive regular information and training on E-Safety issues through the Co-Ordinator at staff meetings.
• All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
• New staff members will receive a copy of the E-Safety policy and Acceptable Use
Agreement and sign an Acceptable Use Agreement.
• All staff are encouraged to incorporate E-Safety into their activities and promote awareness within their lessons.

Handling of E-Safety Issues

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the ICT Co-ordinator to be recorded in the E-Safety log. Issues of a child protection nature will be reported to the designated teacher and dealt with in accordance with the Ashgrove Primary School Child Protection Policy.
Incidents of pupil misuse of technology which arise will be dealt with in accordance with the school's discipline policy. (See Positive Behaviour Policy)

E-safety and Pupils

E-safety will be discussed with pupils at the start of the year when they receive their Acceptable Use Agreement. (see Acceptable Use Policy) This should be discussed as a set of rules that will keep everyone safe when using technology in school.
Activities throughout the school year including Internet Awareness Day and visits from the PSNI will refresh E-Safety and further pupils' understanding.
Pupils will be informed that all network and Internet use is monitored.

E-Safety and Parents

The Ashgrove Primary School E-Safety policy will be published on the school website and parents will be encouraged to read the document. Parents will be required to read the Acceptable Use Agreement for pupils and sign this agreement following discussion with their child.
Ashgrove Primary School will look to promote E-Safety awareness within the school community which may take the form of parents' information evenings, information leaflets or links on the school website.

E-Safety and Staff

All staff will be introduced to the E-Safety policy and its importance explained. Staff will be asked to read and sign the Acceptable Use Agreement for Staff which focuses on E-Safety responsibilities in accordance with the Code of Conduct for employees set out in the Staff Handbook. (see Acceptable Use Policy)

Staff should be aware that all Internet traffic and email is monitored, recorded and tracked by the C2K system.

The Internet

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

Networks

Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse.

Parental permission is sought from parents before pupils access the Internet.

Use of a non C2K wireless network for use with iPads in school is provided by an external Internet provider. This network has appropriate filters applied for use by staff and pupils and use of iPads will only be carried out under staff supervision.

Connection of mobile phones or personal computers to the wireless network is not possible.

Teaching and Learning

Internet use:

• The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.

• Educating pupils on the dangers of technologies that may be encountered outside school will be discussed with Key Stage 2 pupils through Internet Awareness Day and liaison with the PSNI through BEESAFE campaign.

• Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/guardian, teacher/trusted member of staff.

• The school Internet access is filtered through the C2k managed service.

• No filtering service is 100% effective; therefore, all children's use of the internet is supervised by an adult.

• Use of the internet is a planned activity. Aimless surfing is not encouraged.

Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

• Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
• The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
• Children will be taught to be 'Internet Wise'. They will be made aware of Internet
Safety Rules and encouraged to discuss how to cope if they come across inappropriate material.

E-mail:

• Pupils may only use C2k e-mail accounts on the school system.
• Pupils must immediately tell a teacher if they receive an offensive e-mail.
• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
• The forwarding of chain mail is not permitted.
• Children will not always be 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 will be supervised by the teacher.

School Website

The Ashgrove Primary School website promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimize 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
Names and images are kept separate – if a pupil is named their photograph is not used and vice-versa
The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff

Social Networking:

- The school C2k system will block access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of cyber-bullying to the school.
- School staff will not add children as 'friends' if they use these sites.
  (See Social Media Policy)

Password Security

Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
All pupils are provided with an individual login username and password.

Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

Mobile Phones

Ashgrove Primary School does not allow the use of mobile phones by children in school or on school trips. It is important to be aware of the safety issues regarding mobile phones which now increasingly have Internet access.
Staff use of mobile phones, only when necessary, should be discreet. Mobile phones should not be used in the classroom setting and should not be visible to pupils throughout school. (see Mobile Phone Policy)

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained for 3 months*), without permission, except where disclosed to the Police as part of a criminal investigation.
We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with taking digital images and sharing on the Internet.

- When using digital images, staff informs and educates pupils about the risks associated with taking, use, sharing, publication and distribution of images. In particular, they should recognize the risks attached to publishing their own images on the Internet e.g. Social Networking websites.
- The school gains parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school;
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those image.
- We will also ensure that when images are published that the young people cannot be identified by the use of their names, unless prior consent has been obtained.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- The use of digital / video images plays an important part in learning activities.
- The school will comply with the General Data Protection Register (introduced May 2018) by requesting parents' permission when their child starts school Year 1, permission will last until the student leaves school, unless a parent / carer provides a written withdrawal of taking images of members of the school.

Cyber-bullying

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Messaging Apps and Forums – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people. Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.
- Incidents of cyber–bullying will be dealt with in accordance with the School Anti-Bullying Policy. (See Anti- Bullying Policy)

The Data Protection Act

The school is working towards GDRP compliant status (September 2017).

The school has a Data Protection Policy and staff are regularly reminded of their responsibilities. In particular, staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimizing 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" 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, it is advisable that:

- the device is password protected
- 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

See GDPR Policy for Parent/Staff