MEADOW BRIDGE PRIMARY SCHOOL

'OPENING DOORS OF OPPORTUNITY TOGETHER'

ONLINE SAFETY POLICY

APRIL 2023

ONLINE SAFETY POLICY

Rationale

> *"All schools should have their own Online Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. Online 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"*
>
> ***DENI Online Safety Guidance, Circular number 2013/25***

It is the responsibility of the school's 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 school intends 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.

New technologies have become integral to the lives of children and young people in today's society, both within schools and their lives outside school. The Internet and other digital technologies are powerful tools which open new opportunities for everyone. With these opportunities we also have to recognise the risk associated with the online world.

> *"We want pupils to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so, they need to know how to protect themselves.'*
>
> ***DENI Online Safety Guidance, Circular number 2016/27***

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.

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 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 2012**

The main areas of risk for the School can be categorised as the **Content, Contact and Conduct** of activity.

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.

Contact

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

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.
- Inappropriate behaviour towards others.

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 eg Positive Behaviour, Child Protection, Anti-Bullying, Acceptable Use, Mobile devices, and 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.

Roles and Responsibilities

Online Safety Co-Ordinator who is also our ICT Co-Ordinator

The ICT Co-Ordinator will lead the Online Safety section in a Safeguarding Team meeting, take day-to-day responsibility for Online Safety issues, and have a leading role in establishing and reviewing the school's policies/documents.

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 for staff.
- Liaise with C2K and technical staff.
- Ensure Classnet Filtering is up-to-date.
- Liaise with the EA and DENI on Online Safety developments.
- Receive reports of Online Safety incidents and create a log of incidents to inform future Online Safety developments.
- Meet with Senior Management to investigate abuse of social network sites by pupils.
- Attend relevant meetings with Board of Governors.
- Discuss current issues, review incident logs.
- Monitor and report to Senior Management any risks to staff of which the Online Safety Co-Ordinator is aware.

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

The Child Protection Officer (and their deputy) 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.

Safeguarding Team

The Safeguarding Team provides a consultative group that has representation from the school community, with responsibility for issues regarding Safeguarding and child protections. This includes 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.

Team members:

- ICT Co-Ordinator.
- The Designated Child Protection Teacher.
- Child Protection Governor.
- Principal.

Members of the Safeguarding Team will assist the ICT Co-Ordinator 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 pupils, about the Online Safety provision.
- Monitoring improvement actions identified through audit.

The Principal and Senior Management

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 ICT Co-Ordinator.

The Principal and ICT Co-Ordinator 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 Senior Management are responsible for ensuring that the ICT Co-Ordinator 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.

Network Managers

The ICT Co-Ordinator will monitor that Classnet and 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 Classnet Filtering is up-to-date.
- 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 carry out their Online Safety role effectively, and to inform and update others as relevant.

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 Co-Ordinator.
- Digital communications with students (email/Virtual Learning Environment (VLE) should be on a professional level only, carried out using official school systems - C2k and Classnet. 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 organised by the school

Professional Development for Teaching and Support Staff

Training will be offered as follows:

- All new staff will receive Online Safety training as part of their Induction Programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policy.
- A programme of Online Safety training will be made available to staff as an integral element of CPD. Training in Online Safety will be supported within the PRSD or EPD process and where staff have identified a need.
- Staff will be made aware of the importance of filtering systems. They will also be warned of the consequences of attempting to subvert the filtering system.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.

Pupils

Pupils are responsible for ensuring that:

- They use the school ICT systems in accordance with the Acceptable Use Policy. They are expected to sign the pupil agreement before being given access to school's systems.
- They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.
- They understand the importance of reporting abuse, misuse, or access to inappropriate materials and know how to do so.
- They know and understand school policies on the use of mobile phone, digital cameras and hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- Pupils are introduced to email and taught about the safety and 'netiquette' of using e-mail both in school and at home.
- They understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Online Safety Education for Pupils

Online Safety education for students will be provided in the following ways:

- A planned Online Safety programme will be provided as part of ICT/PDMU/other lessons and will be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school. KidsSMART, ThinkUknow, Be Internet Legends resources from the Child Exploitation, Online Protection (CEOP) and Google/Parent Zone are just some of the resources which may be used as a teaching tool.
- Pupils will be taught in all relevant lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet.
- Pupils will be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet, and mobile devices both within and outside school.
- Where pupils are allowed to search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and should be directed/guided to pre-checked websites.
- Pupils will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the Online Safety Policy outlined by the school.

Parents and carers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.
- online communication with staff.
- their children' s personal devices in the school.
- the Acceptable Use Policy is signed annually by parents/carers.

Parents'/Carers' Training and Support

Parents and carers have an essential role in the education of their children and in the monitoring and regulation of the children's online behaviour. The school recognises that some parents may under-estimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will seek to provide information and awareness to parents and carers through:

- A section of the school website providing links to external sites such as CEOP and Digital Parenting.
- Letters, website page, annual advice sheet on Online Safety.
- Any updates/guidance will be delivered to parents through email, Meadow Bridge News, or other relevant channels.
- Online Safety Guidance will be delivered through key events eg P7 Parent/Pupil Information Evening, Safer Internet Day.

Community Users

Community Users who access school systems as part of the wider school provision will be expected to agree to the school's Acceptable Use Policy before being provided with access to school systems and sign AUP sheet.

Education for the Community

The school will provide opportunities for members of the community to gain from the school's Online Safety knowledge and experience through:

- Providing, where possible, family learning courses in use of new digital technologies, digital literacy and online safety signposting to other community sessions.
- The school website.
- Supporting community groups on request.

Current Practice

Communication

- The official school email service may be regarded as safe and secure. Staff and pupils should therefore use the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Email communications with parents and/or pupils should be conducted through the following school email systems '@c2kni.net'. Personal email addresses should not be used.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, or bullying in nature, and must not respond to any such communication.
- Any digital communication between staff and parents/carers – email and Seesaw must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Networking

School endeavours to deny access to social networking sites to pupils during school hours. Staff may use Seesaw to disseminate information to pupils outside of school.

- The school will provide training in the appropriate use of social networking/for teaching and learning purposes.
- Training will include: acceptable use; social media risks; checking of settings; data protection reporting issues; legal risks.
- Staff should adhere to the social networking/communication guidance provided by the school.
- Staff will receive advice in the appropriate use of social networking in their private life.
- Older students should be made aware of the appropriate and safe use of Social Networking and the relevant age guidance for these platforms.
- Staff and pupils should report any incidents of cyber-bullying to the school.
- Further information is provided to staff during in-service training [also see the 'Social Media Policy' for appropriate use].

Pupils' Use of Personal Devices

- The use of mobile phones and smart watches (specifically models which can take photos or record audio) by pupils is not permitted on the school premises during school hours. If a mobile phone is needed for after school, then it should be brought to the school office/class teacher where it will be kept safely until home time. A letter from a parent/carer, requesting that the mobile may be brought to school must accompany the phone.
- Rules for Acceptable Use of the Internet are discussed with pupils and are prominently displayed in classrooms. In addition, pupils follow a programme of online safety awareness.
- Pupils are only allowed to bring their own digital devices into school or on school trips if permitted to do so by their class teacher. On these occasions they must abide by the Acceptable Use Policy and sanctions such as being asked to delete photos/videos, etc, or being banned from Internet usage will apply if the policy is not adhered to.
- Staff should not use personally-owned devices, such as mobile phones or cameras or smart watches (with the necessary capabilities), to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone in case of emergency, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

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 by the Support Provider for 28 days), without permission, except where disclosed to the Police as part of a criminal investigation.

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 inform and educate pupils about the risks associated with taking, use, sharing, publication, and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet, eg Social Networking websites. Children are told of the age limits to social networking sites and parents are provided with an advice sheet annually.
- 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 and an annual update is carried out through digital permission in the Parent Information Pack.
- 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 images.
- School will also ensure that when images are published the young people cannot be identified by the use of their names/surnames.
- 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.

Teaching and Support Staff: Password Security

Password security is essential for staff, particularly as they are able to access and use student 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.
- Further information is provided to staff during INSET training.

Students: Password Security

- Students are expected to keep their passwords secret and not to share with others, particularly their friends.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers, or others.
- Pupils are taught about appropriate use of passwords.

Cyber-Bullying

Cyber-Bullying can take many different forms and guises including:

- Email - nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms - 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 bios, or pretending to be someone online without that person's permission.
- Incidents of cyber-bullying will be dealt with in accordance with the School's Anti-Bullying Policy.

The Data Protection Act

Staff are regularly reminded of their responsibilities with regard to data protection. In particular, 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' 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 and the data is securely deleted from the device in line with school policy once it has been transferred or its use is complete.

Technical Framework

Filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed.

The responsibility for the management of the school's filtering policy is held by the Senior Leadership Team.

The Senior Leadership Team manage the school filtering by:

- Monitoring the use of Classnet and reports of the use of C2K which are available on request.
- Keeping records and logs of changes and of breaches of the filtering systems.
- Reporting these changes and breaches to the ICT Co-Ordinator.

Staff and pupils have a responsibility:

- To report immediately to ICT Co-Ordinator any infringements of the school's filtering policy of which they become aware, or any sites that are accessed, which they believe should have been filtered.
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials

Auditing and Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- Safeguarding Team.
- ICT Co-Ordinator.
- Principal.
- Governors.
- External Filtering Provider/PSNI on request.

Actions and Sanctions

Sanctions for the misuse of technology are outlined in the Acceptable Use Policy and our Positive Behaviour, Child Protection, and Anti-Bullying policies and may be applied as appropriate.