Date Ratified by Board of Governors : 10 January 2019

E-SAFETY POLICY

Date Ratified by Board of Governors : 10 January 2019

Olderfleet Primary School
E-Safety Policy

Context
This policy is based on and complies with DENI Circulars:

- 2007/1 Acceptable Use of the Internet and Digital Technologies in Schools
- 2011/22 Internet/e-Safety
- 2013/25 Internet/e-Safety
- 2015/21 School Obligations – Information Governance and C2k Access to SIMS Data
- 2016/26 Effective Educational Uses of Mobile Digital Devices
- 2016/27 Online Safety

This document sets out the policy and practices for the safe and effective use of the Internet and related technologies on Olderfleet Primary School. It also links to Article 17 from the UN Convention on the Rights of the Child which states:

'You have the right to get information that is important to your well-being from radio, newspaper, books, computers and other sources. Adults should make sure information you are getting is not harmful, and help you understand the information you need.'

What is e-Safety?
E-Safety is short for electronic safety. This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology as well as collaboration tools and personal publishing.

E-Safety in School

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

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 children into contact with people from all sectors of society and with a wide range of materials, some of which could be unsuitable.

The rapidly changing nature of the Internet and new technologies means that e-safety is an ever growing and changing area of interest and concern. This e-safety policy reflects this by keeping abreast of changes taking place. Schools have a duty of care to enable pupils to use on-line systems safely.

This e-safety policy operates in conjunction with other school policies:

- Positive Behaviour
- Child Protection/Safeguarding
- Anti-Bullying
- Acceptable Use of the Internet and Other Digital Technologies
- Mobile Phones and Other Related Technologies.

E-Safety must be built into the delivery of the curriculum. Using ICT is a compulsory cross-curricular element of the NI Curriculum and schools must ensure acquisition and development of these skills by pupils.

This policy highlights the need to educate pupils about the benefits and risks of using technology and provide safeguards and awareness for users to enable them to control their online experiences.

E-Safety in Olderfleet Primary School depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Sound implementation of e-safety policy in both administration and curriculum including a secure school network design and use
- Safe and secure Internet provision by C2K

Care and Responsibility

New technologies have become integral to the lives of children in today's society both within schools and outside. The Internet and other technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion, provide creativity and stimulate effective learning. They also bring opportunities for staff to become more creative and productive in their work. All users should have an entitlement to safe Internet access at all times in school. With these opportunities we also have to recognise the associated risks.

The use of these exciting and innovative tools in schools and at home has been shown to raise educational standards and promote pupil achievement. However they can also place users at risk within and outside school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to or loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate contact or communication with others, including strangers
- Cyber-bullying
- Access to unsuitable video or internet games

- An inability to evaluate the quality, accuracy and relevance of information
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development

As it is impossible to eliminate the risks completely it is therefore essential through good educational provision to build pupils' resilience to any risks to which they may become exposed so that they have the confidence and skills to deal with any scenario which may arise.

In Olderfleet Primary School we understand the responsibility to educate pupils in e-safety issues. We aim to teach pupils appropriate behaviours and critical thinking to enable them to remain safe when using the Internet and related technologies, in and outside the classroom.

Roles and Responsibilities

As e-safety is an important aspect of Child Protection/Safeguarding Children the school's e-safety team, principal and Board of Governors have the ultimate responsibility to ensure the policy and practices are embedded and monitored. It is the role of the e-safety coordinator and the e-safety team (including the ICT Coordinator and C2K managers) to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. This team has the responsibility for leading and monitoring the implementation of e-safety throughout the school.

The e-safety coordinator (Mr B Harvey) and the principal (Mr S Livingston) have the responsibility to update the SMT (Senior Management Team) and BoG (Board of Governors) with regard to e-safety and all governors should have an understanding of the issues relevant to the school in relation to local and national advice.

Responsibilities of the E-Safety Coordinator

The E-Safety Coordinator is responsible to the principal and BoG for the day-to-day issues relating to e-safety.

The E-Safety Coordinator:

- Leads the E-Safety Team
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Provides training and advice for staff
- Liaises with EA and CCEA
- Receives reports of e-safety issues and creates a log of incidents to inform future e-safety developments
- Reports regularly to the SMT
- Receives appropriate training and support to fulfil the role effectively

- Has responsibility for passing on requests to C2K for the blocking/unblocking of internet sites
- Maintains an e-safety log book indicating any occasions where the school has used its powers of search and deletion of electronic devices

The BoG:

- Are responsible for the approval of the policy and reviewing its effectiveness. The BoG should receive regular information about e-safety incidents and monitoring reports.

The Principal:

- Is responsible for ensuring the safety (including e-safety) of all members of the school, though the day-to-day responsibility for e-safety is delegated to the e-safety coordinator.
- The Vice-Principal (if not the e-safety coordinator) should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (refer to disciplinary procedures and/or Child Protection/Safeguarding Children policies).

Teaching and Other Staff

- Have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- Have read, understood and signed the school's Acceptable Use of the Internet Policy for Staff
- Report any suspected misuse or problem to the school's e-safety coordinator
- Embed e-safety guidance into the curriculum and other school activities as appropriate.

E-Safety Skills Development for Staff

E-Safety training is an essential of staff induction and should be part of continuous professional development. Through this policy we aim to ensure that all reasonable actions are taken and measures put in place to protect all users.

- All staff will receive regular information and training on e-safety issues through the e-safety coordinator at staff meetings
- All staff must be 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 the misuse of technology by any member of the school community
- All staff are encouraged to incorporate e-safety into their activities and promote awareness within their lessons
- New staff members will receive a copy of the e-safety policy and be asked to sign an Acceptable Use of the Internet agreement
- Staff who request enhanced internet access on the C2K network will be informed of the appropriate use

Handling of E-Safety

Issues of misuse and/or access to inappropriate material by any user should be reported as soon as possible to the e-safety coordinator (Mr B Harvey) who will record the incident in the e-safety log, giving details of the time, website, etc.

Issues of a child protection nature should be reported to the designated teacher (Mr D Kyle) or any other member of the Safeguarding Team (Mrs E Brownlees and Mr S Livingston) who will deal with the issue in accordance with the Child Protection/Safeguarding Policy.

Incidents of pupil misuse of technology will be dealt with in accordance with the Positive Behaviour/Discipline Policy. Pupils must be made aware that misuse of the Internet may lead to access being denied.

A record of serious incidents will be kept in the Child Protection/Safeguarding Book in a locked drawer in the principal's office.

The E-Safety Log Book will be made available to the:

- SMT
- Principal
- BoG
- E-Safety Team

E-Safety Team

The E-Safety Team consists of:

- Mr B Harvey — E-Safety Coordinator; ICT Coordinator and C2K Manager
- Mr D Kyle — Vice-Principal; Designated Teacher Child Protection
- Mr S Livingston — Principal
- Mrs E Brownlees — Deputy Designated Teacher Child Protection
- Mr G Knox — BoG

Illegal or Inappropriate Activities

The school believes that the activities listed below are inappropriate (and on occasions illegal) within a school context and that users should not engage in these activities when using school equipment or systems (both inside and outside school). Users should not visit internet sites, make, post, upload, data transfer, communicate or pass on any material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images (Illegal – The Protection of Children Act 1978); grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- Possession of pornographic images (illegal – Criminal Justice and Immigration Act 2008); criminally racist material in UK; to stir up religious hatred or hatred on the grounds of sexual orientation (illegal – Public Order Act 1986)
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm

- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable use of equipment provided by the school:

- Using school systems or equipment to run a business
- Use systems, equipment, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by C2K
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties without the necessary licensing permissions
- Revealing or publishing confidential or proprietary information (e.g. financial or personal information, databases, computer or network codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Online gambling and non-educational gaming
- Use of personal social networking sites or profiles for non-educational purposes

If staff suspect misuse might have taken place but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in an appropriate manner and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour or disciplinary procedures.

E-Safety and Pupils

Pupils need to know how to cope if they come across inappropriate material situations online. E-Safety will be discussed with pupils on an ongoing and regular basis. This should be discussed as a set of rules that will keep everyone safe when using technology in school. It will be discussed as they accept the My School log in agreement. Pupils sign a Code of Safe Practice (see Appendix 1)

Activities throughout the year including Internet Awareness Day and visits from the PSNI (KS2) and NSPCC will refresh e-safety and further pupils' understanding.

Pupils in KS2 (Y6 and Y7) will also use the Cyber Café/Think U Know resources as part of their PDMU programme.

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 Staff Code of Conduct. Staff should be aware that all internet traffic (including email) is monitored, recorded and tracked by the C2K system.

At the discretion of the principal, staff can be given enhanced internet access to allow the use of websites for streaming of videos (e.g. YouTube) for educational purposes only. When staff have been given enhanced internet access they must ensure that no pupil is given access to a computer or other device such as an iPad that they are logged onto so that the pupil will not be able to access sites that may contain inappropriate material.

Staff should always ensure that internet searches involving sites that have been granted enhanced access to should not be carried out when children can view e.g. on a computer screen or an IWB (interactive whiteboard). The use of such sites should only take place after the content has been checked to ensure that pupils are not exposed to inappropriate material.

E-Safety and Parents

The E-Safety Policy will be published on the school website and parents will be encouraged to read the document. Olderfleet Primary School will look to promote e-safety awareness within the school community which may take the form of information evenings for parents/carers, information leaflets and/or links on the school website.

Information for parents is available on the Think U Know website: www.thinkuknow.co.uk

Data may be shared with other agencies. Parents are made aware who the school may share data with in the Privacy Notice.

The school uses electronic means of communication with parents. This may include use of emails to send notes and Friday Letters, Facebook for information and sharing of news about the school, See Saw for the sharing of photos and exchanging information between parent and teacher and Twitter. By interacting with parents in this way, pupils may see that social media can be extremely positive when used in a responsible manner.

Teaching and Learning – Internet Safety

Staff and pupils accessing the internet via the C2K network will be required to authenticate using their C2K username and password. This will provide internet filtering via the C2K Education Network.

Access to the internet via C2K is fully auditable and reports are available to the school principal.

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 of school will be discussed with pupils in an age appropriate way on a regular basis with teachers and other agencies (e.g. PSNI CASE project)
- 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 made aware of where to seek advice or help if they experience problems when using the internet and related technologies i.e. parent/guardian, teacher, Childline

- The school's internet access is filtered through the C2K managed service
- No filtering is 100% effective therefore all children's use of the internet in school is supervised by an adult
- Use of the internet should be a planned activity. Aimless surfing is not encouraged. Children are taught to use the internet in response to a need e.g. researching a question that arisen from work in class
- Pupils will be taught what internet use is acceptable and what is not and be 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 (Internet Safety Rules will be displayed in classes) and encouraged to discuss how to cope if they come across inappropriate material

Email Use

- C2K recommends that all staff and pupils should be encouraged to use their school email system for school business; it is strongly recommended not to use home email accounts for school business
- The C2K filtering solution provides security and protection to C2K email accounts by offering scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content
- If pupils are given access to email in school they may only use C2K email accounts
- Pupils must immediately tell a teacher if they receive an offensive email
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission
- The forwarding of chain mail by staff or pupils is not permitted
- Pupils will not always be given individual email addresses. In some instances pupils may have access to a group email to communicate as part of a school project. Messages sent and received in this way will be supervised by the teacher

School Website

Olderfleet Primary School's website promotes and provides information about the school and may showcase aspects of school life. In order to minimise risks of any images of pupils on the school website the following steps are taken:

- Group photographs are used where possible with general labels/captions
- Photographs of pupils on the school website may only be published if permission has been granted by the parent/carer
- Names and images are kept separate e.g. if a pupil is named their image is not used
- The website does not include addresses, telephone numbers, personal email or any other personal information about pupils or staff

Social Networking

Social networking is largely integrated into everyday life and use of social networking sites is commonplace with the result that the lines between school, work and personal life are blurred. To protect staff, pupils and the reputation of the school the following guidelines should be followed:

- The school C2k system denies access to social networking sites; staff are advised not to add pupils as 'friends' if they use these sites
- Staff should not use school systems or equipment to engage in personal social activities e.g. Facebook, Twitter, blogging, wikis, etc. This inappropriate use may be treated as a disciplinary matter
- If staff use social media sites for personal use they are reminded that they have a responsibility to ensure they are posting comments or images that are not detrimental to their position as a member of staff of Olderfleet Primary School, the privacy or rights of other staff or pupils and the reputation of the school. A common sense approach to the use of social media sites is recommended
- Pupils and their parents/careers are advised that the use of social network sites outside of school is inappropriate for primary aged pupils. However, we accept that as some pupils will still use them they will be advised never to give out personal details of any kind, to set and maintain maximum privacy levels and deny access to unknown individuals
- A definition of cyber bullying is provide in the school's Anti-Bullying Policy and staff are made aware that pupils may be subject to cyber bullying via electronic methods both in and out of school
- Pupils are asked to report any incidents of cyber bullying to the school

Password Security

- Staff are provided with individual usernames and passwords which they are encouraged to change periodically. Login details should not be shared with pupils and should be changed should it appear pupils have worked out a staff password
- All pupils are provide with an individual username and password
- Pupils are not permitted to deliberately access files on the school area which belong to any other users
- Staff area/folders are the individual responsibility of staff to ensure and protect the security and confidentiality of the school network

Mobile Phones and other Electronic Devices (including (BYOD) Bring Your Own Devices)

It is important to be aware of the safety issues regarding mobile phones and other devices with internet access. For this reason Olderfleet Primary School has a specific policy on the acceptable use of mobile phones and related technologies.

Pupils are strongly discouraged from bringing phones or electronic devices into school unless a prior agreement has been made with a member of staff. Pupils will only have the ability to personally access the school network using a BYOD when permission has been granted by a member of staff.

Staff members should refrain from using mobile phones or similar technology when in contact with pupils unless prior permission has been granted.

Staff should not use their personal mobile phones or electronic devices to take photographs of pupils without good reason and if they have to the photographs must be removed from the staff member's phone at the earliest convenience and the incident reported to the principal.

Access to the internet on such non-C2K devices should be for school related business only and is only available through the C2K Guest Access which is subject to C2K's filtering system.

Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. Cyber bullying can take different forms including:

- Email – nasty or abusive emails which may also include viruses or inappropriate content
- Instant Messaging and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity
- Social Networking Sites – includes the posting or publication of nasty or upsetting comments
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites
- Mobile Phones – abusive texts, video or photo messages; sexting; inappropriate images transmitted to other people
- Abusing Personal Information – posting of photos, personal information, fake comments and blogs or pretending to be someone online without that person's permission

Whilst cyber bullying may appear to provide anonymity for the bully, most messages can be traced back to the creator and pupils should be reminded that cyber bullying can constitute a legal offence. While there is no specific legislation for cyber bullying the following may cover some elements of cyber bullying behaviour:

- Pupils are encouraged to report incidents of cyber bullying to school and if appropriate the PSNI to ensure that matter is appropriate addressed and the behaviour ceases
- A record is kept of all incidents of cyber bullying in the school's e-safety log to allow the e-safety team to monitor the effectiveness of the school's preventative activities and to review and ensure consistency in investigations, support and sanctions

Network Access

Internet access for all staff and pupils is through the filtered service provided by C2K.

Acceptable Use of the Internet Policy for Staff

The C2K computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management.

The school's e-safety policy has been drawn up to protect all parties – pupils, staff and the school.

The school reserves the right to examine and delete any files that may be held on its computer system and to monitor internet sites visited and emails sent and received.

Staff should read and sign a copy of the Internet Use Agreement for Staff.

Date Ratified by Board of Governors : 10 January 2019

Policy Review

This e-safety policy and its implementation will be reviewed annually and updated when new technologies are introduced and after a risk assessment has been completed.

Signed:

_____ (Principal)

_____ (Chair of Board of Governors)

Date Policy Reviewed:_____

Appendix 1

Olderfleet Primary School

ICT Code of Practice Agreement for Pupils and Parents

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will access the system with my login and password, which I will keep secret.
- I will not access other people's files without permission.
- I will only use the computers for school work and homework.
- I will not bring software or disks/CDs into school without permission.
- I will ask permission from a member of staff before using the Internet.
- I will only e-mail people I know, or my Teacher has approved.
- I will not open e-mails sent by someone I don't know.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number, or arrange to meet someone.
- I will report any unpleasant material or messages sent to me.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not use Internet chat-rooms in school.
- I will never give out personal information or passwords.

Signed (Parent): _____ Date: _____

Signed (Pupil): _____ Date: _____