WHEATFIELD
PRIMARY & NURSERY SCHOOL
Believe ⋆ Achieve ⋆ Succeed

Wheatfield Primary School E-Safety Policy

(Electronic Safety Policy)

Updated October 2022

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 and 2013/25 on Internet /E-Safety. This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Wheatfield Primary School. It also links to Article 17 from the UN Conventions 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 the information you are getting is not harmful, and help you find and understand the information you need."

Care and Responsibility

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 information and communities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times. With these opportunities we all have to recognise the risks associated with the internet and related technologies.

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, 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 context
- Use 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 and individuals consent or knowledge
- Inappropriate communications/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 all 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 Wheatfield Primary School we understand the responsibility to educate out pupils in E-Safety issues. We aim to teach pupils appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

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 E-Safety Co-ordinator (Ms Waugh) and the E-Safety Team 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/Principal has 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.

E-Skills Development for Staff

- All staff will receive training on E-Safety issues through the Co-ordinator
- All staff will 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 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.
- Staff members will receive a copy of the E-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.
- In light of the new filtering on the C2K network staff members who have been granted enhanced internet access will be informed of the appropriate use.

Handling of E-Safety Issues

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the E-Safety Co-Ordinator (Ms Waugh) 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 Wheatfield Primary School Child Protection Policy.

Incidents of pupil misuse of technology which arise will be dealt with in accordance with the Wheatfield Primary School Positive Behaviour Policy.

E-Safety and Pupils

Pupils need to know how to cope if they come across inappropriate material or situations online, E-Safety will be discussed with pupils on an on-going and regular basis. This should be discussed with the pupils in an age appropriate way as a set of rules that will keep everyone safe when using technology in school. E-Safety will be discussed with pupils at the start of the year when they receive their Acceptable Use Agreement. It will also be discussed as they accept the agreement through their MySchool log in.

Activities throughout the school year including Internet Awareness Week and visits from the PSNI will reinforce E-Safety and further pupils understanding.

E-Safety and Parents

Parents will be made aware of the Wheatfield Primary School E-Safety Policy and will be encouraged to read the document. Wheatfield Primary School will look to promote E-Safety awareness within the school community which may take the form of parents' information sessions and information leaflets.

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 focused on E-Safety responsibilities in accordance with the Code of Conduct. Staff should be aware that all Internet Traffic and email is monitored, recorded and tracked by the C2k system.

Networks

Pupil access to the Internet is through a filtered service provided by C2k, which should ensure educational use made of the resource is safe and secure, protecting users and systems from abuse.

Connections of iPads are through the controlled C2k Guest wireless network and is subject to the same level of filtering as the main school system.

Staff should always ensure that no pupil is given access to a computer that they are logged on. Staff should ensure that any internet searches not be carried out when connected to a projector.

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.

Internet Security

Staff and pupils accessing the internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering vas the C2k Education Network solution

Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school Principal.

Connection of non C2k devices to the Internet e.g. iPads through the controlled C2k guest wireless network and is subject to the same level of filtering as the main school system.

Internet Use

- The school will plan and provide opportunities within a range of curriculum area 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 by teachers and other agencies e.g. PSNI
- 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 e.g. parents/carer, school staff/ worry box
- The school internet access is filtered through the C2k managed service. No filtering 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 and as an aid to learning, e.g. a question which has arisen from work in class
- 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' and therefore good online citizens , and are encouraged to discuss how to cope if they come across inappropriate material

E-Mail Use

C2k recommends that all staff should be encouraged to use their C2k email system for school business. **It is strongly advised that Staff should not use personal email accounts for school business.**

Pupils will not always be given individual C2K e-mail addresses. In some instances they may have success to e-mail to communicate as part of a particular project. Messages sent and received in this way will be supervised by the teacher.

Pupils must immediately tell a member of staff if when using their C2K e-mail address (if activated) if they receive an offensive e-mail.

Pupils may not use personal e-mail accounts on the school system.

The forwarding of chain mail by staff or pupils is not permitted

School Website

Wheatfield Primary School's website promotes and provides up-to-date information about the school and showcases 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
- Only photographs of children with parental/carer consent will appear on the school's website.
- Name will be included with photographs on the website only if parent/carer permission has been given;
- The website does not include home addresses, telephone numbers, personal e-mail or any other personal information about pupils or staff.
- The point of contact to the school i.e. school telephone number, school address and email address.

Social Networking

- The school C2k system will block access to social networking sites
- Pupils and parents/carers 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 personal profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are asked to report any incidents of cyber-bullying to the school.

To protect staff, pupils and the reputation for the school the following guidelines should be followed:

- Staff should not use school systems to engage in personal social media activities.
- 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 staff member of Wheatfield Primary School, the privacy or rights of pupils or the reputation of the school. Images may include photographs from staff gatherings that could be misinterpreted and present the staff or the school, in a negative light.
- Staff and pupils are advised that it is not acceptable or school policy for them to be friends on social network sites (e.g. Facebook). **Staff must not request to be friends or accept requests to be friends with pupils, past pupils or parents/carers of the school on any such site.** This is good practice and in line with Child protection/safeguarding children.
- Under no circumstances should offensive comments be made about work colleagues on the Internet. This may amount to cyber-bullying or defamation and could be deemed a disciplinary matter.

Password Security

Staff 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, and should be changed if it appears pupils have worked out an adult's password.

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 and other electronic Devices

It is important to be aware of the safety issues regarding mobile phones and other devices which now increasingly have Internet access. For this reason Wheatfield Primary School has a specific policy on the Acceptable use of mobile phones and related technologies.

Pupils are not allowed to bring such devices into school and will not have the ability to personally access the school network. If mobile phones or other devises are brought into school by pupils, it is our policy that they should remain switched off during the time the pupils are on school premises. Any mobile devised brought in by pupils should be left in the school office and will be returned to them at the end of the school day.

If photographs of pupils are being used by staff for lessons, presentations etc. they should be stored as much as possible on the C2k system. If however, staff are working on school related activities on personal computers, any photographs stored should be kept to a minimum and transferred to the school's network as soon as possible. Photographs stored on a teachers personal computer for school purposed should be deleted as soon as possible after they are no longer required or transferred to the schools C2K 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. Pupils engaging in cyber bullying may be dealt with in line with the school's 'Positive Behaviour Policy' and 'Anti Bullying Policy'.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses on 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, videos 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 ad 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 their creator and pupils should be reminded that cyber – bullying can constitute a criminal offence. While there is no specific legislation for cyber – bullying, the following may cover different elements of cyber – bullying behaviour:

It is important that pupils are encouraged to report incidents of cyber – bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

A record is kept of all incidents of cyber – bullying in the school's e-Safety log. This allows the schools e-safety team to monitor the effectiveness of the school's preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

Network Access

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.

Acceptable Internet Use 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-the students, the staff and the school.

The school reserves the right to examine and delete any files that may be hold on it computer system or to monitor any Internet sites visited.

Staff should read and sign a copy of the school's Acceptable Internet Use Agreement for Staff and return it to the Principal.

Policy Review

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

Acceptable Use Agreement for Staff/Volunteers

In line with Wheatfield Primary School's e-safety policy I understand:

The schools E-Safety Policy has been drawn up to protect all parties. This policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my personal equipment in school or in situations related to my employment by the school.

- All internet activity should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- I must not engage in any on-line activity that may compromise my professional responsibilities or bring the name of the school into disrepute
- Users are responsible for all e-mail sent
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials, such as pornographic, racist or offensive material is forbidden
- When using the C2K system there is a log of my internet searching history
- I should immediately report, to the ICT coordinator, any damage or faults involving equipment or software, however this may have happened

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

NAME: ____________________________________

SIGNED: __________________________________

DATE: _____________________________________

Updated October 2022

WHEATFIELD
PRIMARY & NURSERY SCHOOL
Believe ⋆ Achieve ⋆ Succeed

Acceptable Use of the Internet:

Guidelines for Pupils

Children should be taught from N–P7 that they are responsible for their use on the Internet in school and that they should use it in a safe, responsible and appropriate manner. The following guidelines are shared and discussed with the pupils in an age appropriate way.

Staff should continually teach and stress the importance of safe use of the internet.

WHEN USING THE C2K SYSTEM PUPILS SHOULD:

- Only use their own login username and password
- Keep their username and password private
- Use the internet for school/educational purposes only
- Tell a member of staff if they see anything that they consider inappropriate or receive messages they do not like
- Only send e-mail or any other form or electronic communication in school when directed by the teacher
- Understand that if they consistently choose not to comply with these expectations they will be warned and subsequently may be denied access to Internet resources
- Understand that the school may check their computer files and may monitor the Internet sites they visit
- Never access other people’s files without their permission
- When logged on, not leave their computer unattended
- Never change or delete other people’s files without their permission
- Not being in memory devise from home to use in school unless given permission by a member of staff
- Never provide personal information such as telephone numbers and addresses when using the Internet
- Not use any personal electronic devices I have in my permission within school to access the internet or any messaging services

Pupils should be made aware that:

They are not to damage any school ICT equipment including any resources in the ICT Suite.

That if they deliberately break these rules they could be stopped from using the Internet/ school ICT resources and their Parent/Guardian will be informed.

Updated October 2022