



E-Safety Policy

This document complies with the DENI Circular 2016/27 on 'Online Safety'. Our eSafety policy is an important element of the overall Safeguarding of our pupils. Elements of this document are relevant to both our Child Protection and Anti-Bullying Policies.

September 2017



Context

This policy outlines how the staff and pupils of The Good Shepherd Primary School will approach and use the internet and related technologies in a safe and effective way.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning through devices such as the iPad. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- iPads
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

We want our pupils to have access to the benefits of learning, exploring and connecting online in a safe and secure way. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

The Internet is 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.

Key Concerns

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons.

Children should be taught that:

- people are not always who they say they are.
- "Stranger Danger" applies to the people they encounter through the Internet.
- they should never give out personal details
- they should never meet alone anyone contacted via the Internet
- once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published



for an adult audience and is unsuitable for children e.g. materials with a sexual content.
to express extreme views, e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.
containing misleading and inaccurate information, e.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children should be taught:

- that information on the Internet is not always accurate or true.
- that they should question the source of information.
- how to respond to unsuitable materials or requests and
- that they should tell a teacher/adult immediately.

Excessive Commercialism

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

Children should be taught:

- not to fill out forms with a lot of personal details.
- not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

In The Good Shepherd we understand the responsibility to educate our 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.

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 Leader of ICT to keep abreast of current E-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. Pupil's welfare around digital technologies is the responsibility of anyone who comes in contact with them in the school or on school organized activities. The Leader of ICT has responsibility for leading and monitoring the implementation of E-Safety throughout the school. The Principal/Leader of ICT 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.

Writing and Reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to and used in conjunction with other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying. This policy should not be seen as exclusive.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body.

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.**

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

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 sign a copy of the Acceptable Use Agreement.
- All staff are encouraged to incorporate E-Safety into their activities and promote awareness within their lessons in accordance with the ICT schemes of work.

Handling of E-Safety Issues

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the Leader of ICT to be recorded in the E-Safety log. Issues of a child protection nature will be reported to our designated teacher, Mrs Finnegan, and dealt with in accordance with the Good Shepherd 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.

E-safety and pupils

E-safety will be discussed with pupils at the start of the year when they receive their Acceptable Use Agreement. 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 eSafety week and Safer Internet Day will refresh eSafety and further pupils' understanding.

Pupils will be informed that all network and Internet use is monitored.

E-Safety and Parents

The Good Shepherd 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.

The Good Shepherd Primary School will look to promote E-Safety awareness within the school community which may take the form of parents' information evenings, information leaflets and on the school website.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use there. Guidelines include

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as iPads and smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.



- Take an interest in what children are doing.
- Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner.
- Know the SMART tips (see later)
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant.
- Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

The school website contains links to sites like CEOP's, ThinkUKnow, Childline, and the CBBC Web Stay Safe page.

Parents/Guardians are required to make a decision as to whether they consent to images of their child being taken/used on the school website.

Networks

The school Internet access is filtered through the C2k managed service and Classnet. Connection of mobile devices or personal computers to the wireless network is not permitted.

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 is done informally when opportunities arise and formally as part of the e-Safety curriculum set out as part of the new UICT guidelines. Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also 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, or an organisation such as Childline/CEOP.

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 permitted. Children are taught to use the Internet as part of a planned teaching activity.

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, all as part of the new UICT requirements

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules (S.M.A.R.T) and are encouraged to discuss how to cope if they come across inappropriate material.

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

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 planned and agreed activity. Messages sent and received in this way will be supervised by the teacher.

School Website/Social Media

The Good Shepherd 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 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
- Full names and images are kept separate – if a pupils full name is used their photograph is not, and vice-versa unless prior permission is given by a parent.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff

Written permission from parents or guardians will be obtained before photographs of pupils are published on the school Website or in local social media. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/carers may withdraw permission, in writing to the Principal, at any time.

Social Networking:

- The school C2k and Classnet systems 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.

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



The Good Shepherd Primary School does not allow the use of mobile phones by children in school or on school trips. Any pupil with a mobile phone in school must leave it into the school office at the beginning of the school day.

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.

Memory Pens

The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material. Staff should not store pupils' personal data and photographs on memory sticks.

Managing Video-conferencing

Videoconferencing will be via the C2K or Classnet network to ensure quality of service and security. Video-conferencing will be appropriately supervised and parents informed before the commencement of the activity. Any video-conferencing undertaken will be part of agreed teaching and learning programmes agreed by the school.

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. Any such attempt will be treated as a breach of school rules with appropriate sanctions. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network and SIMS system.

Handling e-Safety Complaints:

Complaints of Internet misuse by pupils will be dealt with by the Leader of ICT and/or member of SLT. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the e-Safety incident logbook.

Any complaint about staff misuse must be referred to the Principal. Complaints of a child protection nature must be dealt with in accordance with school Child Protection Policy and procedures.

Pupils and parents will be informed of the complaints' procedure.

Communicating the Policy

Introducing the e-Safety Policy to pupils

e-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year.

Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week eSafety Week and Safer Internet Day. Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety Policy

All staff will be given the School e-Safety Policy and its importance explained. Any information downloaded must be respectful of copyright, property rights and privacy. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

Monitoring and review



This policy is implemented on a day-to-day basis by all school staff and is monitored by the Leader of ICT. This policy is the Governors' responsibility. The e-Safety policy and its implementation will be reviewed annually. They will do this during reviews conducted between the Leader of ICT and Designated Child Protection Co-ordinator.

Please discuss these rules with your class regularly and display them



Be Smart on the internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk

THINK U KNOW

www.kidsmart.org.uk

KidSMART Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Childnet International is a registered charity in England and Wales. Registered number: 1095964. Registered office: 100 Brooklands Drive, Basingstoke, Hampshire, RG24 0AA.



clearly in your room.

Rules for Responsible Internet Use (FS/KS1)

Pupil Agreement

Good Shepherd Primary School has computers and iPads with Internet access to help your learning. The rules below will help keep you safe when using the Internet. Please read them carefully.

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers or iPads.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer, iPad and other equipment.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer/iPad.

Pupil Name: _____

As the parent or legal guardian of the pupil named above, I grant permission for my son/daughter to use the Internet under supervision. I have talked to my child about these rules and confirm that they will follow them. ☐

I give permission for my child's photograph to be taken and used in school, on school publications, on the school website. ☐

Pupils may take part in activities with other organisations e.g. Ulster Orchestra, Colin Neighbourhood Partnership, who wish to take photographs for use on their own social media. Your child's safety is paramount therefore the school will only associate with organisations which have been vetted through child protection safety checks.

Please tick if you give permission for your child's photo to be taken and used on **responsible** social media such as these. ☐

I give permission for my child to participate in video conferencing for educational purposes e.g. collaborating with other schools. ☐

Signed (parent):



Rules for Responsible Internet Use (KS2)

Good Shepherd Primary School has computers and iPads with Internet access to enhance your learning. The rules outlined below will help keep you safe when using the Internet. Please read them carefully and complete the permission form below.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Using the Computers/Devices

- I will not enter the folders or files of anyone else;
- I understand that the teachers can monitor my use of the computers
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will not alter computer or iPad settings.
- I will not download any software or apps without teacher instruction.
- I will only use the printer when instructed to do so and after I have checked my work.
- I will take care of the ICT equipment I have been asked to use.
- I know that if I break the rules I might not be allowed to use the computer, iPad or other equipment.

Using the Internet

- I will ask permission from a teacher before using the Internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not complete and send emails without permission from my teacher;
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will be polite and responsible when I communicate with others; I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- When I am using the Internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Please sign and return the attached form to show your agreement.

You may keep this sheet for your information.

Good Shepherd Primary School's KS2 Acceptable Use for Internet and digital technology



Pupil's name: _____ Class teacher: _____

As a school user of the Internet, I have read and agree to follow the school rules on its' use. I will use the network in a responsible way and observe all the restrictions explained to me by my school.

Pupil's name [Print]: _____

Pupil's name Signature: _____

Date: _____

As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet, including Email. I understand that pupils will be held accountable for their own actions. I also understand that some of the materials on the Internet may be unsuitable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information. ☐

I give permission for my child's photograph to be taken and used in school, on school publications, on the school website. ☐

Pupils may take part in activities with other organisations e.g. Ulster Orchestra, Colin Neighbourhood Partnership, who wish to take photographs for use on their own social media. Your child's safety is paramount therefore the school will only associate with organisations which have been vetted through child protection safety checks. Please tick if you give permission for your child's photo to be taken and used on **responsible** social media such as these. ☐

I give permission for my child to participate in video conferencing for educational purposes e.g. collaborating with other schools. ☐

Parent/Guardian name [Print]:

Parent/Guardian name Signature:

Date: _____



This policy is to provide guidance and accountability to members of staff at Good Shepherd Primary school who use the Internet and who have been issued with an iPad.

Acceptable Use of Internet

- The 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 Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.
- The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.
- Staff must sign a copy of this Acceptable Internet Use Statement and return it to the Principal before the beginning of the school term.
- 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.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. 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

User Responsibilities

- The iPad screen is made of glass and is therefore subject to cracking and breaking if misused.
- Users must use the protective cases provided for their iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Do not subject the iPad to extremes of temperature.
- Do not store or leave unattended in vehicles.
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad as safe and secure as possible.
- Users are advised to set a 4 digit pin to maintain the security of their iPad. This must be held by you and not divulged to pupils or other members of staff.
- Users will not remove or change profile settings on your device or attempt to "jailbreak" the device.

Safeguarding and Maintaining as an Academic Tool



- Use of the iPad should be considered the same as any other technology tool provided by the school.
- Users must abide by the schools Internet AUP when using the iPad.
- Users may not photograph any other person without that person's consent
- Photographs of children must be in line with school policy- they must be downloaded/removed from the device before it is taken home.
- Users are advised not to store personal documents such as video or audio material other than that which is directly related to school needs.
- To not allow any pupil to use the iPad for any purpose except for curricular purpose under a controlled environment in the presence of a member of staff.
- Users must not "sync" the school device with a home computer.
- Users are to ensure personal web searches are deleted before using the iPad in class.

Apps

- To ensure all apps downloaded are suitable for school use.
- To ensure that all apps meet with the criteria of the schools e-safety policy.
- To only use the school account for all app purchases on the device.
- To keep a list of apps downloaded.
- To inform ICT-coordinator when apps are purchased at a cost.

Lost, Damaged or Stolen iPad

- If the iPad is lost, stolen or damaged, the ICT Coordinator, or principal must be informed immediately

Please read and sign below:

I have read, understand and agree to abide by the terms of the **iPad Acceptable Use Policy**.

I have received a school ipad and charger.

Name:

Signature:

Date: