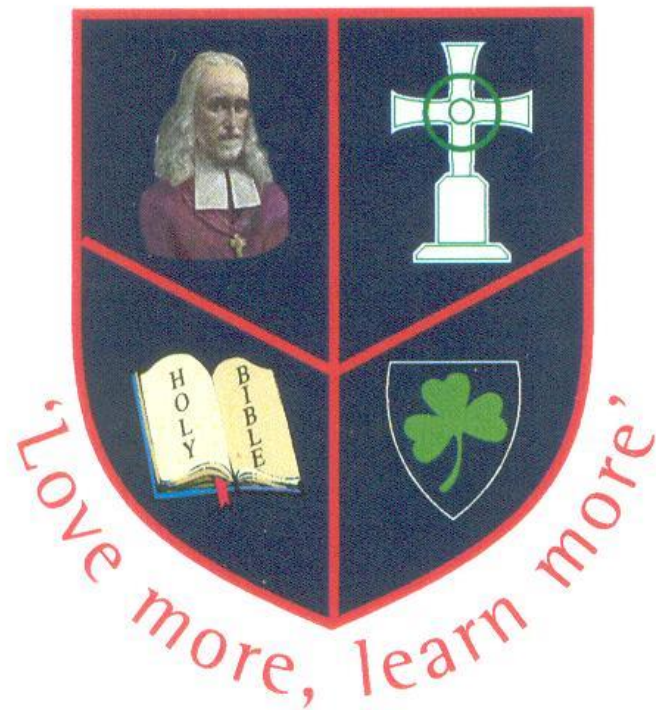


St Oliver Plunkett PS and Nursery Unit



E-Safety Policy

Rationale

Boards of Governors have a duty to:

- Safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries N. I. Order 2003).
- Determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries N.I. Order 2003).

In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils: these will serve to reassure parents and guardians.

In St Oliver Plunkett's Primary School, we understand the responsibility to educate our pupils in E-Safety issues. We aim to teach them 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. Our E-Safety Policy reflects the importance we place on the safe use of information systems and electronic communications. It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions.

E-safety encompasses internet technologies and electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

E-Safety (Electronic Safety)

- 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;
- prepares pupils to recognise unsafe situations and how to respond appropriately.

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. (See Appendix for key concerns).

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 the changes taking place. The school has a duty of care to enable pupils to use on-line systems safely. This e-Safety policy contains aspects in relation to use of the internet, use of mobile phones and use of digital/photographic images of children. It is largely based on DENI Circular 2007/1 "Acceptable Use of the Internet and Digital Technologies in Schools", DENI Circular 2011/22 "Internet Safety" and DENI Circular 2013/25 "e-Safety Guidance". It should also be read in conjunction with the School's Safeguarding Policies.

ICT is a compulsory element of the NI Curriculum and schools must ensure acquisition and development by pupils of these skills. The Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. Our school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

The DENI circular 2007/01 states that:

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

This document sets out the policy and practices for the safe and effective use of the Internet and digital technologies in St Oliver Plunkett's Primary School and Nursery Unit. We aim to develop systems of safety awareness, so that users can easily adapt their behaviours and become responsible users of any new technologies. The policy has been drawn up by the staff of the school under the leadership of Mrs Kearney (Principal) and ICT Co-ordinator (Mrs McTague). It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested. The policy and its implementation will be reviewed annually.

E-Safety in St Oliver Plunkett's Primary School and Nursery Unit 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 secure school network design and use.
- Safe and secure internet provision by C2k.

Roles and Responsibilities

As E-Safety is an important aspect of Child Protection / Safeguarding Children within the school, the Principal, ICT Co-ordinator and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

ICT Co-ordinator:

- is responsible for the day-to-day issues relating to Online Safety and has a leading role in establishing and reviewing the school Online Safety policies/documents,
- ensures that all staff are aware of the procedures that need to be followed in the event of an incident,
- provides training and advice for staff,
- receives reports of Online Safety incidents and creates a log of incidents to inform future developments,
- receives appropriate training and support to fulfil his/her role effectively,
- passing on requests for blocking/unblocking to the Capita helpdesk.

The Board of Governors:

- are responsible for the approval of this policy and for reviewing its effectiveness. The governors should receive regular information about Online Safety incidents and monitoring reports.

The Principal:

- is responsible for ensuring the safety (including online safety) of members of the school community.
- and the Vice-Principal 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 staff disciplinary procedures, and/or Child Protection/Safeguarding Children Policy.

Teaching and Support Staff must:

- have an up-to-date awareness of online safety matters and of the current school E- safety policy and practices;
- embed online safety issues into the curriculum and other school activities as appropriate;
- 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 ICT co-ordinator;

E-Safety Skills' Development for Staff

- All staff will be given the School E-Safety Policy and its application and importance explained.
- All staff will receive regular information and training on E-Safety issues through the co-ordinator at staff meetings.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members will receive a copy of the E-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.
- All staff are encouraged to incorporate E-Safety into their activities and awareness within their lessons.

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and/or used on the school website, Seesaw and Facebook page.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- The school will communicate and promote relevant E-Safety information through newsletters, Seesaw and the school website / Facebook page.
- Internet issues will be handled sensitively and parents will be advised accordingly.

Parents should remember that it is important to promote E-Safety in the home and to monitor Internet use.

- Keep the computer/iPad/tablet in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones/games consoles/tablets.
- 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.
- 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.
- Keep passwords private at all times and do not allow their children access to these.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach E-Safety.
- Key E-Safety messages will be reinforced annually through Safer Internet Week.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- 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/carer, Class Teacher/trusted member of staff.
- E-Safety is a focus in all relevant areas of the curriculum.
- The school Internet access is filtered through the C2k managed service. No filtering service is 100% effective; therefore all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

- Pupils will be helped to understand and act in accordance with the ICT Acceptable Use Agreement of Pupils.
- 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 are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.
- When using digital images, pupils are taught about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff act as good role models in their own use of ICT.

E-mail:

- Pupils may only use approved e-mail accounts in school, e.g. C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive 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 are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

- The school network system will block access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils will be advised not to place personal photos on any social network space. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location e.g. house number, street name or school.
- Our pupils are asked to report any incidents of bullying to the school.

- Pupils will be advised that sending abusive messages or images in any online format will be considered as bullying and will be dealt with accordingly.
- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT coordinator.
- Staff **should not use school systems** to engage in **personal** social media activities, i.e. Facebook, Twitter, blogging, wikis etc. This inappropriate use of social media sites 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 staff member of St Oliver Plunkett's Primary School, the privacy or rights of pupils or the reputation of the school. Images may include photographs from staff parties that could be misinterpreted and present the staff or the school, in a negative light. **A common sense approach to the use of social media websites is recommended.**
- School staff will not add children as 'friends' if they use these social networking sites.

Mobile Technologies:

- 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.
- Pupils are not allowed to bring personal mobile devices/phones to school.
- Staff should not use personal mobile phones during designated teaching sessions.

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, Seesaw or Facebook page. 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, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used on the School Website or Facebook in association with photographs.

- Teachers will endeavour to take pictures of groups or group activities, however individual pictures will be used from time to time.
- Staff are allowed to take digital/video images to support educational purposes following the E-Safety policy. Images should only be taken on school equipment, e.g. school cameras, iPads.
- The principal and ICT coordinator has the authority to refuse, withdraw or delete an inappropriate image or article from the school website / Facebook page.
- Pupil's work will be displayed on our school website on occasions.
- Any article/image on our website remains the property of our school.

Authorising Internet access:

All staff must read and sign the 'Acceptable Use Agreement For Staff' before using any school ICT resource.

- All access to the internet will be supervised.
- The school will take all responsible precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Therefore, the school can not accept liability for the material accessed or any consequences resulting from Internet use.
- Complaints of Internet misuse will be dealt with.
- Any complaint about staff misuse must be referred to the Principal.
- E-Safety rules will be posted in classrooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

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.

Cyber Bullying:

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communications both in and out of school. This form of bullying is also referenced to within our school's overall Anti-Bullying and Pastoral Care Policies. 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. It is important that pupils are encouraged to report incidents to both school and, if appropriate, to the PSNI to ensure the matter is properly addressed and the behaviour ceases. We will also keep a record of cyber-bullying incidents to monitor the effectiveness of our preventative activities and to review and ensure consistency in our investigations, support and sanctions.

Handling E-Safety Complaints:

- Issues of internet misuse and the access to any inappropriate material should be reported immediately to the school's ICT Co-ordinator and recorded.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator in the school's E-Safety log, giving details of the site and the time. A record of very serious incidents will be kept in the locked Child Protection/Safeguarding Children cabinet within school.
- Any complaint about staff misuse must be referred to the Principal.
- Pupils and parents will be informed of the complaints' procedure.
- To deal with any incidents of technology abuse by pupils the school's Positive Behaviour Policy will be followed. Pupils must be made aware the repeated misuse of the internet may lead to their access to it being denied. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed.
- Where the incident involves child abuse, the Designated Teacher for Child Protection/Safeguarding Children in the school must be notified and the school will follow procedures set out in the Child Protection/Safeguarding Children Policy.
- Harassment of another person using technology, or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), poses a threat to their physical and emotional safety, and may have legal consequences. For these purposes, it is also essential that evidence of misuse is secured. If the school identifies a suspect device (containing for instance indecent images or offences concerning child protection), it will not be used or viewed and advice will be sought from the P.S.N.I.

Communicating the Policy:

Introducing the E-Safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. The SMART rules will be continually reinforced throughout the school year in all aspects of the curriculum when using the Internet. Specific lessons on E-Safety will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times.
- 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 could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop/iPad 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 ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the ICT Co-ordinator/Team and Senior Leadership Team.

Appendix

Use of Internet 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.
- That “Stranger Danger” applies to the people they encounter through the Internet.
- That they should never give out personal details or
- That they should never meet alone anyone contacted via the Internet, and
- That 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.

Materials may express extreme views e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.

Materials may contain 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.
- To 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.