e-Safety Policy

January 2016

Omagh Integrated Primary School and Nursery

e-Safety Policy

This policy complies with the following Department of Education Northern Ireland (D.E.N.I.) Circulars:

- 2007/1: Acceptable Use of the Internet and Digital Technologies in Schools
- 2011/22: Internet Safety
- 2013/25: E-Safety Guidance

Introduction

E-Safety is short for Electronic Safety. Our school understands, and takes seriously, its responsibility to educate the school community in E-Safety issues. We aim to highlight appropriate and acceptable digital behaviour, enabling our staff and pupils to remain both safe and legal when using the internet and other digital technologies, in and beyond the context of the classroom.

The internet, and other technology-based tools, are now essential means of communication. These very powerful resources open up new prospects for communication and collaboration and they can enhance and potentially transform teaching and learning when used effectively and appropriately.

Omagh Integrated Primary School and Nursery is embracing the internet, and other new and emerging digital technologies, which have become integral to all our lives, as they bring with them many opportunities for everyone in our school community. We believe that these digital technologies are innovative tools and that they offer vast, diverse and unique resources to enrich our teaching and learning, raise educational standards and promote achievement. The internet, and other digital technologies, are widely accessible within our school and we aim to use them to promote educational excellence through facilitating resource sharing, innovation and communication.

The use of new technologies such as this can pose many risks and dangers within and outside of school. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills and an understanding of their appropriate and effective use both in and outside of the classroom.

The care, welfare and safety of every child and employee are of fundamental importance to us all in Omagh Integrated Primary School and Nursery. It is our aim, therefore, through excellence in our educational provision, to build the resilience of everyone within our school community 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.

Scope

This policy covers the acceptable use of the internet by all school stakeholders, including teachers, support staff, Governors, pupils, parents, supply staff, work experience and teaching practice students and volunteers.
E-Safety covers not only internet technologies but also electronic communications via, for example, mobile phones, games consoles and wireless technology.

Objectives

The objectives of this policy are to:

- Develop awareness of how to respond to risks appropriately.
- Ensure that internet use is monitored and managed appropriately.
- Ensure efficient, moral and legal use of the internet resources available within school.
- Ensure our pupils and staff understand and use new technologies in a positive way.
- Ensure that everyone within our school will benefit from the teaching and learning opportunities, offered by the school's internet and digital resources, in a safe and effective manner.
- Help our school community to feel confident online when they use internet technologies and electronic communications.
- Safeguard, as far as possible, our school community in the digital world.
- Support the development of safer online behaviours both in and out of school.

Links with other Policies

- This policy on E-Safety operates in conjunction with other school policies including Anti-Bullying; Positive Behaviour; Child Protection; I.C.T.; policy for acceptable use of mobile phones and related technologies; Acceptable use of the internet and Social Media.

Roles and Responsibilities

Board of Governors and Principal

- Take ultimate responsibility for internet safety issues within the school.
- Be proactive ambassadors of an internet safety culture within the school. Actively promote safe and acceptable working practices for all staff and pupils.
- Ensure that the I.C.T. Team / Co-ordinator have the appropriate authority, and adequate allocated time, to effectively carry out their duties with regards to E-Safety.
- Ensure that the school has a policy on the safe, healthy, acceptable and effective use of the internet and other technology tools, and that the E-Safety policy is embedded and monitored throughout the school.
- Allocate appropriate funding to support internet safety activities throughout the school.
- Be aware of and understand the issues relevant to our school in relation to local and national guidelines and advice.
- Ensure that any incidents, in which internet safety is breached, are responded to in an appropriate and consistent manner.

I.C.T. Team / I.C.T. Co-ordinator

- Establish and maintain a safe Information and Communication Technology (I.C.T.) learning environment within the school.
- Lead and monitor the implementation of E-Safety throughout the school.
- Keep abreast of current E-Safety issues and guidance.
- Lead in the creation of a staff professional development programme. Provide staff with regular information and training on E-Safety issues.
- Update Senior Management and Governors with regard to E-Safety.

- Establish and maintain a school-wide E-Safety programme.
- Maintain an overview of E-Safety activities across the school.
- Develop a parental awareness programme on E-Safety.
- Maintain a log of all incidents relating to internet safety in school.
- Document the location of all internet-accessible computers and devices within the school.
- Record issues of internet misuse and access to any inappropriate material, in the school's E-Safety log. Refer matters of a child protection nature to the Designated Teacher.
- Develop and review appropriate E-Safety policies and procedures.
- Disseminate the E-Safety policy to all members of the school community.
- Ensure that Acceptable Use Agreements are signed by all members of the school community.
- Liaise with outside agencies, as appropriate.

Designated Teacher for Child Protection

- Have a proactive role in E-Safety issues.
- Support the I.C.T. Team / Co-ordinator in the development and maintenance of appropriate policies and procedures relating to E-Safety and child protection.
- Liaise with the I.C.T. Team / Co-ordinator when matters of a child protection nature have been recorded in the school's E-Safety log.
- Develop and maintain knowledge of E-Safety, particularly with regard to child protection issues.
- Ensure that pupils who experience problems when using the internet are appropriately supported.
- Know about organisations providing advice, referrals or resources on issues relating to E-Safety and child protection.

Curriculum Leaders

- Consider if there are E-Safety measures pertinent within the teaching of their subject, and communicate these to the I.C.T. Team / Co-ordinator.
- Ensure that E-Safety messages are embedded within the context of their curriculum area.

Teaching Staff

- Develop and maintain knowledge of E-Safety issues.
- Implement school policies and procedures on E-Safety.
- Ensure any instances of internet misuse, whether accidental or deliberate, are dealt with through the proper channels.
- Provide the necessary support to pupils who experience problems when using the internet.
- Plan classroom use of the internet and I.C.T. facilities to ensure that internet safety is not compromised.
- Embed teaching of E-Safety messages throughout teaching and learning experiences, wherever possible.

All members of the school community

- Maintain an appropriate level of conduct in their own internet use both within and outside school.
- Sign an Acceptable Use Agreement.
- Know what to do in the event of misuse of technology by any member of the school community and know how and when to report an incident of concern.

Sanctions

While use of the internet is a required aspect of the statutory Northern Ireland Curriculum, access to the internet remains a privilege and not a right. This privilege will be given to those who act in a considerate and responsible manner. However, if choices are made not to adhere to these guidelines, and acceptable standards of use are not maintained, the school will respond accordingly to such incidents of misuse, in accordance with the school's disciplinary procedures.

Reporting incidents of misuse

As part of our E-Safety awareness activities within school, all users of I.C.T. will receive guidance on how to seek advice or help if problems are experienced when using the internet and related technologies, and of how to cope in the event of accessing inappropriate material or situations online.

Responding to incidents of misuse

Within Omagh Integrated Primary School and Nursery, we use and maintain a variety of strategies to ensure that the educational use made of the internet, and other digital technologies, within our school is safe and secure. Although we have rigorous measures in place to protect both our school community and our I.C.T. systems from abuse, it must be accepted, however, that, despite our best efforts, these measures will never be completely effective. There may be times when infringements of our policies and procedures could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In this event, we will respond in the ways detailed below.

Level One: Minor incidents

Minor incidents of misuse might include:

- Unauthorised use of non-educational sites during lesson time.
- Unauthorised use of social media.
- Misconduct associated with logging in, such as using someone else's password.
- Unauthorised downloading or uploading of files.

(Please note that this list is not exhaustive. The Principal will categorise incidents, in accordance with further guidance, if and when they occur.)

Responding to minor incidents of misuse

Stage 1:

- Pupils:
    - The incident will be referred to the I.C.T. team / Co-ordinator.
    - The pupil will discuss which aspect(s) of the internet Acceptable Use Policy they have broken. Together with the member of staff, they will reminded about the policy, to refresh their understanding of it. A form will be completed to show that this process has been undertaken.
    - The incident and response will be documented.

- Employees:
    - The incident will be referred to the Principal.

Stage 2:

- If the behaviour is repeated:
- Pupils:
    - The incident will be referred to the Principal.
    - Parents will be contacted.

    - Internet access will be removed from the pupil for one week.
    - The incident and response will be logged.

- Employees:
    - Referral to the Principal, for further action, in accordance with the relevant policies.

Stage 3:

- If the behaviour escalates:
- Pupils:
    - The incident will be referred to the Principal.
    - Internet access will be removed for a minimum of 2 weeks.
    - A letter will be written to parents and they will be asked to come into school to discuss the pupil's breaking of the Acceptable Use Policy. The pupil, Principal, a member of the I.C.T. team and the designated teacher for child protection will attend this meeting.
    - The incident and response will be logged.

- Employees:
    - Referral to the Principal, for further action, in accordance with relevant policies.

<u>Level Two: Incidents involving inappropriate materials or activities</u>

Inappropriate usage might include:

- Hacking.
- Virus attack.
- Online gambling.
- Material that others may find offensive such as hate material, sexist or racist jokes, cartoons, or material which is used in low-level harassment.

(Please note that this list is not exhaustive. The Principal will categorise incidents, in accordance with further guidance, if and when they occur.)

Responding to incidents of inappropriate usage

- These more serious incidents should be immediately reported to the Principal, who will decide on an appropriate course of action.
- Thorough record-keeping and documenting will occur throughout the process.
- It may also be necessary to involve child protection staff to provide follow-up counselling and support to both the victims and perpetrators.
- The I.C.T. team will review internet safety policies as soon as possible after the incident in an attempt to prevent such an incident recurring, debriefing relevant staff accordingly, and providing school-wide training as appropriate.

<u>Level Three: Incidents involving illegal activities</u>

Illegal activities may include:

- The viewing, possession, making and distribution of indecent images of children / adults.
- Serious stalking or harassment facilitated by communication technologies.

(Please note that this list is not exhaustive. The Principal will categorise incidents, in accordance with further guidance, if and when they occur.)

Responding to incidents of inappropriate and illegal usage

- Omagh Integrated Primary School and Nursery regards the discovery of indecent material within the school's network as a very serious situation, which we will report to the P.S.N.I. as required.
- The Principal will contact the Chairman of the Board of Governors, convene the school's Critical Incident Team and contact the E.A. West Critical Incident Team.

Communication with parents and carers

Omagh Integrated Primary School and Nursery believe that effective communication with parents and carers, regarding E-Safety, is vital to ensure the safety and welfare of the children in our care. E-Safety is an excellent and mutually beneficial topic that can encourage home-school links.

Through this E-Safety Policy, and other relevant policies, we will endeavour to communicate with parents, informing them of the precautions the school is taking to ensure a safe I.C.T. learning environment for their children. We will also have made them aware of the standards of behaviour and acceptable use of I.C.T. that their children are expected to abide by when at school.

While in school, school staff will guide pupils toward appropriate and acceptable use of the internet. However, parents and carers should be aware that they are responsible for their children's use of internet resources at home and that they play a crucial role in creating a safe I.C.T. learning environment and culture, through promoting internet safety at home and reinforcing the messages taught in school.

Omagh Integrated Primary School and Nursery will take every opportunity to help parents and carers gain an appreciation of E-Safety and understand these issues through, for example, running workshops or training sessions; distribution of the relevant policies; sharing information on E-Safety via newsletters, letters, literature, website links, etc. and suggesting practical strategies which parents may wish to adopt in the home. We will endeavour to link with our Parents' Council, where possible, to assist with the organisation and promotion of E-Safety events.

Parents and carers will be encouraged to support the school in promoting E-safety practice and to follow the guidelines set out in our relevant policies.

Omagh Integrated Primary School and Nursery will ask parents to sign a Parental Acceptance Form, as part of their child's agreement to follow the school's Acceptable Use Policy on the use of the internet.

Review of policy

This policy will be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to E-Safety or incidents that have taken place.

This policy was reviewed by staff: __November/December 2015

This policy was reviewed by Governors on: __January 2016

Signed: _____ (Chair of the Board of Governors)

Signed: _____ (Principal)

Policy To be Reviewed in 2018

APPENDIX ONE:

STRATEGIES FOR IMPLEMENTING E-SAFETY

Omagh Integrated Primary School and Nursery employ a number of strategies in order to maximise teaching and learning opportunities and reduce risks associated with the internet. These strategies are as follows:

Acceptable Use

- All members of our school community will be reminded that the use of the school's information technology resources is a privilege which can be removed. They will be given clear guidance on the acceptable use of the internet.
- All users will be expected to adhere to a clear Acceptable Use Policy that is reviewed annually. This policy will remind all users of their responsibilities whenever they are using the internet and include generally accepted rules of I.C.T. etiquette.

Anti-Virus

- All workstations connected to the internet have appropriate anti-virus software installed. The anti-virus software is updated regularly.

Awareness Activities

- All within the school community will be encouraged to use the internet in response to a need. Use of the internet within Omagh Integrated Primary School and Nursery is a planned activity and we do not encourage aimless surfing.
- Clear indications, throughout the school community, of how to seek advice or help if problems are experienced when using the internet and related technologies, and of how to cope in the event of accessing inappropriate material or situations online.
- E-Safety will be built into the delivery of the curriculum and we will deliver a comprehensive, consistent and continuing programme of internet safety education throughout the school community.
- Hold bi-annual parents' information evenings. These sessions allow parents to understand the risks posed by a range of internet-enabled hardware, including phones, PCs and gaming consoles.
- Information leaflets.
- Internet Awareness Day (usually takes place each year in February).
- Inviting parents or carers, local business owners or I.C.T. professionals, with a high level of computer literacy and an understanding of E-Safety issues, to assist in delivering E-Safety messages.
- Links on the school website.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation.
- Presentation from organisations, such as the PSNI, on E-Safety.
- Regular updates on E-Safety will be delivered to everyone within our school community.
- In every class, staff will explicitly teach the safe use of the internet.
- As well as being taught as a discrete subject, E-Safety will be embedded into the culture and curriculum of the school.

Chat Rooms

- Access to internet chat rooms will only be permitted for educational reasons.
- Pupils will only have access to discussion forums, messaging or any other forms of electronic communication that have been approved by the school.

- Discussion forums and other electronic communication forums, e.g. Fronter, will only be used for educational purposes and will always be supervised or monitored.

Cyber Bullying

- Omagh Integrated Primary School and Nursery has a zero tolerance approach to cyber bullying.
- This form of bullying will be considered within our anti -bullying and pastoral care policies, as well as this E-Safety policy and other related I.C.T. policies.
- In the event of any cyber-bullying incidents, we will keep thorough records, in order to monitor the effectiveness of our preventative activities, and to review and ensure consistency in our investigations, support and sanctions.

E-Mail

- Omagh Integrated Primary School and Nursery strongly advise that employees should not use home email accounts for school business.
- Pupils will use only approved school or class e-mail accounts. This will be under supervision by, or with the permission of a teacher.

Filtering

- The C2k filtering system is used in order to minimise the risk of exposure to inappropriate material. By default, this system prevents the following categories of websites from being available to our internet users:
    - *Adult:* content containing sexually explicit images, video or text, and the depiction of actual or realistic sexual activity.
    - *Criminal skill / activity:* content relating to the promotion of criminal and other activities
    - *Gambling:* content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice
    - *Hate material:* content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
    - *Illegal drug taking and the promotion of illegal drug use:* content relating to the use or promotion of illegal drugs or misuse of prescription drugs
    - *Violence:* content containing graphically violent images, video or text
- We realise that although thorough, the C2k filtering service, as with any filtering service, can never be comprehensive. If at any time, school employees or pupils find themselves able to access, from within the C2k system, internet sites which they think should be blocked, they will advise the Principal (or, in his absence, the I.C.T. Team / Co-ordinator). The Principal should then report the matter to the C2k Helpdesk and they will implement agreed procedures for handling such issues. These actions will be taken immediately.
- The C2k filtering system also provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.
- Pupils will only use apps on the school iPads. They will not have access to the internet through the C2k managed wireless service.

Mobile / Personal Devices

- The use of devices owned personally by staff and pupils is subject to the same requirements as technology provided by the school.
- When using a school Laptop or other device off the school site, at home or elsewhere, users will still have to abide by the school internet Acceptable Use Policy.
- Control of access to the Wireless network is, at all times, managed by the school.

- Omagh Integrated Primary School and Nursery does not allow the use of mobile phones by children in school or on school trips.
- Pupils must not make use of their own devices to connect to the wireless network.
- The use of mobile phones by employees should be discreet. Mobile phones should not be used in the classroom setting and should not be visible to pupils throughout school.

Password Controls

- Staff and pupils accessing the internet via the C2k Education Network will be required to authenticate using their unique C2k username and password. This authentication will provide internet filtering via 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.
- While normal privacy is respected and protected by password controls, users must not expect files stored on the C2k servers to be absolutely private.

Policies

- We believe that an infrastructure of effective policies and procedures is the backbone to effective practice. Therefore, we have a portfolio of various policies, governing acceptable use of the internet, which are frequently reviewed and updated. These policies will be shared with everyone in our school community.
- All policies have been drawn up to protect the interests of everyone within our school community.
- The policies outline clear guidance that everyone within our school community is expected to adhere to.
- The policies also outline sanctions which will be implemented should individuals choose not to adhere to our guidelines on acceptable use of the internet.
- We will engage in a cycle of creation, maintenance, ongoing review and modification of all internet safety policies and practices.

Professional Development

- E-Safety is an essential element of our on-going staff training and Professional Development programme within Omagh Integrated Primary School and Nursery.

Risk Assessments

- We will perform risk assessments on the technologies available within our school, to ensure we are fully aware of and can mitigate against the potential risks involved with their use.
- The risk assessments will inform teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.

School Website

- The website is regularly checked to ensure that there is no content that compromises the safety of anyone within our school community.
- The publication of student work will be co-ordinated by a teacher.
- Personal information of pupils and employees, including home address and contact details, will be omitted from web pages.
- Pupils will continue to own the copyright of any work published on the school website or the Virtual Learning Platform (Fronter).

Supervision

- All users will be made aware that C2k monitor, record and track all internet based activities and e-mail sent or received. User activity is logged and reports of usage are available to nominated staff within school.

- Internet access for pupils is available only on computers in the classrooms and resource areas. Computers which are connected to the internet will be in full view of people circulating in those areas of the school.
- While using the internet at school, pupils will, where possible, be supervised. However, when appropriate, a pupil may be given permission by a teacher to use the internet and e-mail when completing an individual task. In all cases, pupils will be reminded of their responsibility to use these resources in line with the school policy on acceptable use.

Training

- Everyone within Omagh Integrated Primary and Nursery will be provided with training and guidance in the area of acceptable internet usage.

APPENDIX TWO:

GUIDANCE SHEET FOR INTERNET RESEARCH

- Ensure that you are aware of the relevant internet and e-mail based skills that you are teaching the pupils.
- All web materials should be reviewed and evaluated prior to use with the children.
- to ensure that the content is appropriate.
- Use focused search tasks rather than very open research tasks for younger pupils to ensure that accidental access to inappropriate web sites is reduced.
- Use sites saved to favourites whenever possible to reduce accidental access to other sites.
- Use sites know to be child safe whenever possible.
- Check any open searches you intend to ask pupils to do in advance to ensure you are aware of the risks.
- Minimise the opportunities for any mis-spellings by the children as mis-spellings may cause inappropriate material to be found.
- Ensure you know the procedure to follow if a pupil finds an unsafe site during lesson time.
- Teach pupils what to do if they accidentally find an unsafe site while using the internet.
- Teach pupils not to use any personal information such as name or address at any time when e-mailing or using the internet (e.g. at home or school) and the reasons why this could be unsafe.
- Teach children to involve teachers, parents and carers whenever they are communicating with people they do not know.
- Teach pupils to use the internet responsibly and to speak to their teacher, parents or carers if they feel unsure or unsafe.
- Teach pupils that web sources could be unreliable and inaccurate. Encourage them to check their information against other sources and not to rely on just one information source.
- Supervise pupil use of the internet, e-mail and other digital technologies.
- Ensure parents are made aware of the risks of internet and e-mail use in order that they can take precautions at home.
- Be aware that searches for images may result in unsafe images as pictures are not easy to filter out. Test the search first and check not just the first page/s of returns to be sure.

Additional Advice for Parents with Internet Access at home

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.

2. Parents should agree with their children suitable days/times for accessing the Internet.

3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use.

4. Parents should get to know the sites their children visit and talk to them about what they are learning.

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below).

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities.

7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school they should immediately inform the school.

Further advice for parents is available from the following sources:

- http://www.thinkuknow.co.uk Think u know (a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues)
- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf (Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more)
- http://www.parentscentre.gov.uk/usingcomputersandtheinternet (A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites)
- http://www.bbc.co.uk/webwise (Includes an 'Internet for Beginners' course and a tool for answering your internet related questions)
- http://www.kidsmart.org.uk/ (Explains the SMART rules for safe internet use and lots more besides)
- http://www.ceop.gov.uk/ (The government's Child Exploitation and Online Protection Centre (CEOP))
- http://www.parents.vodafone.com (Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use)