Our Lady's and St Mochua's Primary School

E-Safety Policy

&

Acceptable Use Policy

(Including Acceptable Agreement)

2018

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. 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
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

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.

In Our Lady's and St Mochua's 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.

The Internet – Online Safety (DENI Circular 2016/27 has guided policy as per below)

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. Key Concerns are:

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 will 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.
- P7 participation in the Bee Safe programme covers all of above.

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 will 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 will 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

As e-Safety is an important aspect of strategic leadership 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 ICT Co-ordinator and his/her team to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal/ICT Co-ordinator will update Senior Management and Governors when necessary, with regard to e-safety and all governors will have an understanding of the issues at 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 other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying.

It has been agreed by the ICT Team, Staff, Pupils and Parents and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- All staff 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 receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff incorporate e-Safety activities and awareness within their lessons.
- Both the ICT Coodinator and the Vice Principal have attended Securus Training and Monitor Online Activity within the school.

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/used on the school website.
- 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 relevant e-Safety information through newsletters and the school website.

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

- Keep the computer/mobile device 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.
- 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.

The school will provide e safety workshops for parents periodically. The last workshop took place in November 2013 and was delivered by REAM.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety but a formal approach is adopted via our PDMU Programme.

- 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, teacher/trusted member of staff, or an organisation such as Childline/CEOP.

- The school Internet access is filtered through the C2k managed service.

- C2K defines three types of access;

  Green – accessible to all users

  Amber – accessible to schools'selected groups of users – includes access to youtube, bbc iplayer etc. Mr Farrell will decide on access rites to specific users.

  Red – not accessible to any user

- 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 allowed. 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 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.

- 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 and are encouraged to discuss how to cope if they come across inappropriate material.

- Search engines require careful use and planning/supervision. Children can be bombarded with information and yet fail to find the material they need. Teachers should select the search engine and topic and discuss sensible search words which have been tried out beforehand.

- Children do not need thousands of website addresses. A small appropriate choice is much more effective. Favourites is a useful way to present this choice. Sites should always be previewed and revisited to be checked out. Consider off-line viewing

- Individual e-mail addresses are not considered suitable for children. Class or project e-mail addresses should be used. All incoming and outgoing mail should be checked – children in P6 and P7 may use the C2K email provided for in school emailing only.

- Discuss with pupils the rules for responsible Internet use. It is not enough to protect children from materials, we must teach them to become Internet Wise. Children need to learn to recognise and avoid the risks. Children need to know what to do if they come across inappropriate material or if they are approached by a stranger.

- In preparation for internet use within a lesson teachers should have viewed the site previously to ensure that any content including advertising is appropriate. E.g. If using YouTube teachers are expected to link the clip to an email and open directly from there.

E-mail:

- Pupils may only use 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 C2k 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.
- Our pupils are asked to report any incidents of online bullying to the school.
- School staff will not add children as 'friends' if they use these 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 or other data storage devices taken outside school.
- Pupils are not allowed to use personal mobile devices/phones in school. However, on occasion pupils may be allowed to bring mobile technologies into school e.g. Golden Time, Christmas Toy Day. During these times usage will be closely monitored by the teacher. These devices will not be allowed to access the school network.
- 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

- The school may publish on the school website or in the local newspaper, photographs that will celebrate an individual or group of children's achievements/success.
- The school, having taking advice from the EA Designated Child Protection Officer and in consultation with BOG, staff and parents, will publish photographs using the following guidelines;

  NEWSPAPER: Photographs of an individual/group will be published with full name/s of child/ren so that achievements can be celebrated by wider community, family and friends.

  WEBSITE/FACEBOOK/TWITTER: Photographs of an individual child will be accompanied by first name only e.g. Congratulations to John P6 who won a gold medal at the swimming gala. Photographs of a group of children will also have first names of children only.
- The school principal, Mr Farrell, may also give permission for other bodies to use school photographs/children's photographs to celebrate or publicise their and the school's work.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website/FACEBOOK/Twitter/Newspapers/Other Publications. 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.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.
- Staff will have different internet access restrictions than pupils. This will allow them to access a greater array of teaching and learning materials. These will be in line with the C2K Red, amber and green guidelines.

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 are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Handling e-Safety Complaints:

- Complaints of Internet misuse will be dealt with by the ICT Co ordinator and his team.
- 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 procedures.
- Pupils and parents will be informed of the complaints' procedure.

Additional Information:

The school uses **Securus** to assist in our monitoring of our online activities. Securus monitors the screen display and keystrokes alerting schools that a student may be at risk or in breach of acceptable use. Some of the issues and concerns that Securus detects include;

- Cyberbullying
- Online grooming and child abuse/exploitation
- Depression, self-harm and suicide
- Racial, homophobic and religious harassment
- Use of drugs or weapons
- Attempts to use a proxy bypass to access restricted sites

We also use operate an **Online Safety Risk Register** to record potential breaches of online safety and report such to C2K. We also operate a **Register of Access** to further protect all users. This register outlines who has access to the different pupil and staff data available on the school system.

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/Internet Safety Day.
- Pupils will be informed that network and Internet use will be monitored.
- The school will provide e safety workshops for pupils and parents periodically. The last workshop took place in September 2018 and was delivered by REAM Solutions.

Cyberbullying

Cyberbullying can be defined as using IT, particularly mobile phones and the Internet, to upset someone else. School staff, parents and pupils aim to work together to prevent such behaviour and to act appropriately and effectively when it occurs.
Deliberate abuses which happen outside school, but which impinge upon or affect school pupils and staff, will be dealt with through appropriate disciplinary and, where appropriate, external agency action.

Grooming and images of child abuse

If school staff, parents or pupils suspect or are made aware of any of the following illegal acts, the matter must be reported to the Designated Teacher immediately:

- a child enticed or coerced to engage in sexually explicit conduct on- line
- importing or transporting obscenity using telecommunications public networks

- knowingly receiving images of child abuse whether via the Internet or other digital device (such as mobile phone); these include images which appear to be photographs, whether made by computer graphics or otherwise.

Procedures for reporting and dealing with incidents surrounding breaches in the school's online safety guidelines as outlined in the E Safety Policy will be followed; this will depend on the nature of the incident as to the procedure the school will follow i.e. whether we follow the Safeguarding/Child Protection Procedures or the Managing Behaviour Policy Procedures.

All pupils and staff have signed acceptable use of the internet, school based technology and personal mobile technology as appropriate.

Sanctions

- Sanctions as laid out in the School's Managing Behaviour Policy or Safeguarding/Child Protection Policy (whichever is deemed most appropriate) will be followed when a child deliberately breaks any rules in relation to e safety.
- An 'Online Incident' book is kept in the Principal's Office to record all related incidents and what path was followed in dealing with each case.

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 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:

The school audits their current online safety provision using the 360 degree safe website via fronter. This was last completed in June 2018.

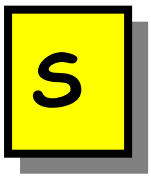
This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

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 and Designated Child Protection Co-ordinator.

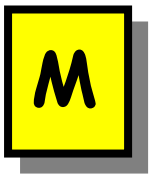
DENI Circular 2016/26, 2016/27 and 2014/14 have been referred to when updating this policy.

Safety Rules for Children

Follow These SMART TIPS



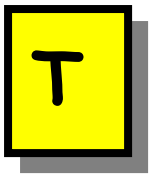
Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!



Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.

Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.

Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Proctection Committees

An Acceptable Use of the Internet

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will use the Internet for research and school purposes only.
- I will only send e-mail (KS2 Only) which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When sending e-mail (KS2 Only) I will not give my name, address or phone number or arrange to meet anyone.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/emails and may monitor the Internet sites that I visit.
- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.
- I understand that if I deliberately break these rules I could be stopped from using the Internet/email and my parents/cares will be informed.

Our Lady's and St Mochua's Primary School

Acceptable Use Agreement
For Pupils

Please complete and return this form to your child's class teacher

Pupil's Name		**Class Teacher**	
As a school user of the Internet, I 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 Name (print)			
Pupil Signature		**Date**	

Parents Name			
As the parent or legal guardian of the pupil above, I give permission for my son or daughter to use the Internet in school in line with the School's E Policy (including Email usage KS2 Only when applicable).			
Parents Name (print)			
Parents Signature		**Date**	

OUR PRIMARY SCHOOL

Acceptable Use Agreement
For Staff

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 should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- 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 is forbidden
- All personnel devices brought into school by staff must not have content that could be deemed inoffensive or be misconstrued in any way.
- Staff may access the school network via their own personal devices in line with this policy for own planning but should use a school designated device for teaching and learning purposes.

Name		
Date		**Signed**

Guidance Material on Internet Safety

http://schoolsl.becta.org.uk

www.ceop.gov.uk

www.thinkuknow.co.uk

Examples of safety rules for children are also available from:

http://www.kented.org.uk/ngfl/policy

Signed:

Chairman of Board of Governors:

Principal: