

St. Teresa's Primary School Lurgan















E-Safety Policy and Acceptable Use Agreement

Contents Page

Introduction	3
E Safety	4
Risks of The Internet	5
Roles and Responsibilities	7
E-Safety Information for Parents/Carers	8
Teaching and Learning	9
Remote Learning	11
Publishing Pupils' Images and Work	12
Policy Decisions	12
Communicating the Policy	13
Appendices	15
- Safety Rules for Children	
- Letter re written permission to use photographs on the school website / press	
- Acceptable Use Agreement for pupils and parents	
- P1 Keeping Safe Form (issued during Induction) Acceptable Internet Use and Photograph permission	
- Foundation and Key Stage 1 Acceptable Use of the Internet	
- Key Stage 2 Acceptable Use of the Internet	
- Staff Agreement Acceptable Use of the Internet	

Introduction





Information and Communications Technology (ICT) covers a wide range of resources from traditional computer-based technologies to the fast evolving digital communication technologies including web-based and mobile learning. Currently some of the internet based and electronic communications technologies children and young people are using, both inside and outside of the classroom, include:

-  Websites
-  Learning Platforms and Virtual Learning Environments (VLE)
-  Email and Instant Messaging
-  Chat Rooms and Social Networking
-  Blogs and Wikis
-  Podcasting
-  Video Broadcasting – Skype / FaceTime
-  Music Downloading
-  Gaming
-  Mobile/Smart phones with text, video and/or web functionality
-  iPads
-  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.

E Safety

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 concerns safeguarding children and young people in the digital world.
-  E- Safety emphasises learning to understand and use new technologies in a positive way.
-  E-Safety is less about restriction and more on education about the risks as well as the benefits so pupils can feel confident online.
-  E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

In St Teresa'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.

Risks of The Internet






The Internet and digital technologies are powerful educational resources they are unique and exciting resources when they are used effectively. The internet 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. Understanding the technology, being a skillful user and displaying safe effective practice is extremely important, teaching effective and safe use is an essential element of the school curriculum. Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe. Pupils need to have the opportunity to avail of all the positive benefits that come from learning, exploring and connecting with each other online. However, in doing so, they need to know how to protect themselves, this education is as important for staff and parents as it is for pupils.

Safeguarding and promoting pupils' welfare around digital technology is the responsibility of everyone who comes into contact with them in the school or on school-organised activities.

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. In St Teresa's children should be taught:

-  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. 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. In St Teresa's 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 by telling a teacher/adult immediately.



Cyber Bullying

We are very aware of the potential for pupils to be subjected to cyber bullying via e.g. email, text or social networking sites. If it takes place within school, cyberbullying will be dealt with in line with the school's overall anti-bullying policy, promoting positive behaviour policy and pastoral care policy. In St Teresa's children should be taught:

-  If they feel they are being bullied by e-mail, through social networking sites, text or online they should always tell someone they trust.
-  Not to reply to bullying, threatening text messages or e-mails as this could make things worse.
-  Not to send or forward abusive texts, e-mails or images to anyone.
-  Keep abusive messages as evidence.

Excessive Commercialism

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

Children will be encouraged to report incidents of cyber-bullying to parents and the school to ensure appropriate action is taken.

Children will be encouraged to use websites such as www.thinkuknow.co.uk to learn how to deal with cyberbullying incidents which may take place in or outside of school

We will keep records of cyber-bullying incidents, if they have occurred within school, to monitor the effectiveness of preventative activities, and to review and ensure consistency in investigations, support and sanctions.

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 Principal & ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The Principal & ICT Coordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.


The Principal updates staff and Governors with regard to e-safety and all governors have an understanding of the issues at St Teresa's 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 Principal, Staff and approved by the Board of Governors. The e-Safety policy and its implementation will be reviewed as appropriate.



E-Safety Skills' Development for Staff

-  All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings as appropriate.






-  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 E-safety Policy Acceptable Use Agreement as part of their induction.
-  All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.
-  Staff are aware of the use of c2k email facility and the policy not to use personal email addresses for school purposes, particularly in relation to children.

E-Safety Information for Parents/Carers

Parents/carers have an important role to play in promoting e-Safety, they are required to read through and sign the Acceptable Use Agreement on behalf of their child, Key Stage 2 children are asked to counter sign this agreement. Parents/carers are encouraged to become involved in e-Safety discussion and activities with 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 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 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 (as shown in the appendix).

- 🏰 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 their own home or at school and that this internet use may not be filtered or supervised.






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 as part of the ICT 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 laptop's / workstations 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 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.


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 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



-  Devices controlled by the C2K network 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 bullying.
-  School staff will not add children as 'friends' if they use these sites.

Personal 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.

-  Key Stage 2 pupils may use a memory stick to save work for school. The memory stick must be for school work only and must not contain any other data or information.
-  Staff should not store pupils' personal data and photographs on memory sticks.
-  Pupils are not allowed to use personal mobile devices/phones in 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.

Remote Learning

In the event of long-term closure, staff at St Teresa's Primary School will continue to provide education and support to our pupils using remote learning.

In this case, learning will be conducted mainly through Seesaw and other C2K supported eLearning and digital platforms. This will allow staff to keep in daily contact, in a professional and confidential manner with parents/pupils in their class.

Teachers will be able to schedule learning in a manner that does not overwhelm or concern pupils. Teaching and learning can be tailored, changed and updated as time progresses, allowing for replication of classroom activity to the best of our ability.





The Principal will monitor each class Seesaw account and other eLearning / digital platforms utilised for remote learning purposes.

Whilst staff are interacting with children away from the school premises, they must continue to adhere to the 'Acceptable Use of the Internet and School Computers', ICT and E-Safety policies and professional standards.

Staff should contact parents through c2k email or Seesaw. All remote communication with students should be done exclusively via approved IT platforms. Never use personal accounts.





In all communications we will adhere to our commitment to maintaining pupil well-being.

Publishing Pupils' Images and Work




-  Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. 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.
-  Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
-  Pupil's work can only be published by outside agencies with the permission of teacher, the pupil or the parents.

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.
-  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.

Password Security

-  Adult users are provided with an individual login username and password, which is changed every three months. 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.

Handling e-Safety Complaints

- Complaints of Internet misuse will be dealt with by the Principal.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Principal 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.

Communicating the Policy



Introducing the e-Safety Policy to pupils

- e-Safety rules will be 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.
- 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 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 Principal.
-  This policy is the Governors' responsibility and they will review its effectiveness as appropriate.

Signed: _____

Chairperson of the Board of Governors

Dated: _____

Appendices

-  Safety Rules for Children
-  Letter re written permission to use photographs on the school website
-  e-Safety agreement for individual pupils eg ipads etc
-  Acceptable Use Agreement for pupils
-  Foundation and Key Stage 1 Acceptable Use of the Internet
-  Key Stage 2 Acceptable Use of the Internet
-  Staff Agreement Acceptable Use of the Internet

Safety Rules for Children

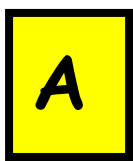
Follow These SMART TIPS



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 Protection Committees

Letter -re written permission to use photographs on the school website / local press

Dear Parents

As part of our E-Safety Policy and Acceptable Use Agreement written permission must be obtained from all parents/guardians before photographs of pupils are published on the school website. In addition, I understand that on occasion my child may be taking part in events which may be publicised in the local press. I understand that on some occasions my child's photograph may also be included in the background of another child's photograph. This consent will be considered valid for the entire period your child attends St Teresa's Primary School.

Please complete the form below and the Acceptable Use Agreement for each child and return to the school office **no later than Friday September**. Please note P5 – P7 pupils (KS2) must also sign the Acceptable Use Agreement.

I give/do not give my permission for my child's photograph and/or work to be published on the school website or in the local press.

I understand pupils' full names will not be used with photographs.

I acknowledge this consent is valid for the entire period of my child's attendance in St Teresa's Primary School unless there is a change in circumstances.

Signed: _____ Parent

_____ Parent

Child's Name: _____

Class: _____

Dated: _____

St Teresa's Primary School Acceptable Use Agreement For Pupils

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

Child's Name: _____ **Class:** _____

As a school user of the Internet, I agree to follow the school rules on Internet 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 Signature (P5 – P7 pupils only)	
Dated:	

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.

Parent's Name (print)		
Parent's Signature		Dated:
Parent's Name (print)		
Parent's Signature		Dated:

P1 Keeping Safe Form

Name of Child _____

Rules for Responsible Internet Use

The school has computers and Internet Access to help our learning. These rules will keep everyone safe and help us be fair to others. Parents are asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- I will only use the computer for school work and homework;
- I will not bring in CDs or memory pens from outside school unless I have been given permission;
- I will ask permission from a member of staff before using the Internet;
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately;
- I understand that if I deliberately break these rules I could be stopped from using the Internet;
- I understand that the school may check my computer files and may monitor the Internet sites which I visit.

My Parents/Guardian and I have read the rules.
I will abide by these rules.

Pupil's Name:

Pupil's Signature:

I have discussed the above rules
of use with my child.

Parent's Name:

Parent's Signature:

Permission to Photograph

I consent for my child's photograph to be taken and used for display/theme purposes, in the local press and for the school website. When a photo is used on the school website, it will be displayed in line with the E-Safety Policy. A photo will not be displayed with the child's full name attached. I understand that on some occasions my child's photograph may also be included in the background of another child's photograph.

Signed _____ (Parent/Guardian) Date _____

St Teresa's Primary School
Acceptable Use of the Internet
Foundation Stage and Key Stage 1 Children

Child's Name: _____ Class: _____

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 use my own login username and password.
- I will not look at, 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 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 understand that if I deliberately break these rules I could be stopped from using the Internet

Signed: _____ Parent

_____ Parent

Dated: _____

St Teresa's Primary School
Acceptable Use of the Internet
Key Stage 2 Children

Child's Name: _____ **Class:** _____

Children should know that they are responsible for ensuring 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-mails 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 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 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/E-mail and my parents/carers will be informed.
- I will not access any Social Media Sites eg Facebook, Twitter etc. while using school computers.

Signed: _____ Child Dated: _____

_____ Parent

_____ Parent

St Teresa's Primary School
Acceptable Use of the Internet and School Computers 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 Acceptable Use Policy has been drawn up to protect all parties – the pupils, 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-mails sent and for contacts made that may result in e-mails being received
- Use of school computer for personal activities such as online purchasing of goods, financial gain, gambling, political purposes or advertising is strictly forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- The same professional levels of language and content should be applied to emails as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Name: _____ Dated: _____

Signed: _____

