Trinity Nursery School

E-Safety Policy
& Acceptable Use Agreement
for Parents
2018-2019

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 using 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 the Schools Community into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. The information contained within this policy is intended as guidance for parents and staff of Trinity.

Key Concerns are:

Potential Contact

Whilst Nursery children will not yet have the skills or access within school they may come into contact outside school 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. For this reason this policy document is intended to guide our parents and prepare them for the opportunities and challenges which lie ahead.
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
- 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 reclaimed.

Inappropriate Content

On 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 groups 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.

As children get older they 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 always 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.

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 Pastoral Care and Child Protection.
It has been agreed and approved by the Board of Governors and will be reviewed annually.

E-Safety Skills Development for Staff

- All staff receives regular information and training on E-Safety issues.
- All staff will be 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 are encouraged to incorporate E-Safety activities and awareness when engaging with the children.
- Parents will receive a copy of this E-Safety Policy.
- Trinity Nursery School will hold an evening session on E-Safety for parents led by a Community Police Officer (PSNI).

E-Safety Information for Parents/Carers

- 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.

Advice to Parents

Parents should remember that it is vital 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. (See Appendix 1)
- 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.
- Be aware of age restrictions in relation to particular websites and games. These have been set for a reason and the content involved is not appropriate for younger children. For example, many social media sites and games allow online interaction between users – if a younger child is accessing these then other users may presume automatically that the child or young person is older.
- Keep up to date. You can get helpful advice (including advice on how to set and manage parental controls on your devices from home) from a number of sites including: www.getsafeonline.org and www.nspcc.org.uk.

Teaching and Learning

Internet use:

- The school Internet access is filtered through the K9 browser
- 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.
- The school will ensure that the use of Internet derived materials by staff 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.

E-mail:

- The forwarding of chain mail is not permitted.

Social Networking:

1. Staff must not access social networking websites for personal use (ie. Non-job related use) during the school day.
2. School staff must act in the best interests of the school and not disclose personal data, information or images about any individual including staff, young people or children that could breach the Data Protection Act 1998.

3. Staff must not make defamatory remarks about the school, it's employees or pupils or conduct themselves in a way that is detrimental to the school.
4. School staff will not add pupils or past-pupils under the age of 18 as 'friends' on social media sites unless they are a relative and of the appropriate age to use the social media site in question.
5. Where staff members communicate with parents, issues regarding any school business should remain confidential and professional and always reflect the best interests of the school.
6. Parent Networking Sites should not be used by the Staff Team. Parents and Staff may raise any concerns through the school's complaints procedures.

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.
- Children are not allowed to use personal mobile devices/phones in school. If phones are brought in to school they will be left in the office for safekeeping and collected by the parent at home time.
- Parents or visitors are not permitted to use mobile phones within the school building.
- Staff should not use personal mobile phones during designated teaching sessions except with the consent of the principal, and staff mobile phones should otherwise be stored in a designated area except with the consent of the principal.

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 and school is notified, in writing, by the parent/carer.
- 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 the pupil and parents.

Outside Photographers

- When commissioning professional photographers or inviting the press to an activity the prior approval of the principal will always be obtained and the staff member organising the event will ensure those attending are clear about expectations of them in relation to child protection.
- Staff will seek confirmation of accreditation by asking the person to produce their professional identification and these details should be recorded in the Visitors Book.
- The principal will inform other staff, parents and children that a photographer will be in attendance at the activity and check that they have signed the consent form, issued at the beginning of the school year, which gives permission for the taking and publication of photographs.
- The principal will not allow unsupervised access to the children or one-to-one photo sessions, nor will approve photo sessions outside the activity.

Policy Decisions:

Authorising Internet access

- Access to the Internet will be supervised.

- All staff must read, agree and sign the school's E Safety Policy.

Wi-Fi

- The nursery has Wi-Fi access which is password protected to ensure authorized access. The password will be change on a regular basis to ensure that security is maintained. It will be for business use only and therefore, the current password will not be shared automatically with staff and parents/carers but only where there is a specific need.

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.
- Children 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 under the Child Protection procedures.
- 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.

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.
- Any laptop or 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.

<u>Social Networking</u>

Staff must not access social networking websites for personal use (i.e. non- job related use) during work time. School staff must act in the best interests of the school and not disclose personal data or information about any individual including staff, young people or children. This includes images. Access may be withdrawn and disciplinary action taken if there is a breach of confidentiality or defamatory remarks are made about the school, staff, young people or children. The school respects an employee's private life. However, it must also ensure that confidentiality and its reputation are protected. Staff using social networking websites in their private life

- must refrain from identifying themselves as working for the school, in a way which has, or may have, the effect of bringing the school into disrepute
- must not identify other school staff, children or young people without their consent;
- must not make any defamatory remarks about the school, its employees, children or young people, or conduct themselves in a way that is detrimental to the school;

- disclose personal data or information about the school, employees, children or young people, that could breach the Data Protection Act 1998, for example, posting photographs or images of children or young people;
- Where staff are contacted by parent/ carer they should bring it to the Principal's attention.
- It is mandatory for staff to re-boot their PC daily with the anti-virus software to ensure that no viruses are present.
- Under no circumstances must games or free issue software be loaded onto school equipment.
- If a specific application programme is necessary for a member of staff's work, then it will be purchased by the school.
- 'Pirate' copies of school owned software for use by other persons either inside or outside the school is an illegal practice.
- Failure to comply with any procedure will result in disciplinary action

The aims and principles of the E-Safety Policy for Trinity Nursery School have been agreed by the staff and endorsed by the Board of Governors. This policy will be reviewed and updated in line with the Policy Review Cycle and in light of any changing guidance or legislation.

November 2017

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 annually.

This E-Safety policy was approved by the *Board of Governors on:*	*Date 16th November 2015*
The implementation of this E-Safety policy will be monitored by the:	*Principal*
Monitoring will take place at regular intervals:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The next anticipated review date will be: **November 2018**	*November 2018*
Should serious E-Safety incidents take place, the following persons and external agencies should be informed:	*Principal and Designated Child Protection Officer, Education Authority .PSNI*

Please remove, sign and return this section to your Class Teacher

ICT and Internet

As the parent or legal guardian of the pupil, I grant permission for my child to use the Internet, when supervised by an adult. I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media at home.

NAME OF CHILD (block capitals) _____

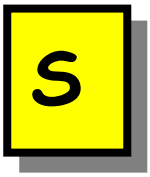
NAME OF PARENT/ CARER (block capitals) _____

Signature: _____ Date: _____

APPENDIX 1

Safety Rules for Children

Follow These SMART TIPS

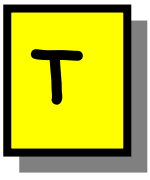


Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!

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

Acceptable Use Agreement For Staff

APPENDIX 2

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 E Safety Policy has been drawn up to protect all parties.

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.

- 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
- Staff should refrain from emailing official information to their personal or home email accounts
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden
- Staff must take care when attaching documents
- Copies of e-mail should be retained where appropriate (as e-mail is a form of documentation which could be 'discoverable' in legal proceedings)
- Because of potential virus infection and consequent damage to the business, staff must not load any software into any computer without the prior approval of school management
- Approval will only be given after virus checking. Virus protection software is maintained and periodically updated
- It is mandatory for staff to re-boot their PC daily with the anti-virus software to ensure that no viruses are present

- Under no circumstances must games or free issue software be loaded onto school equipment
    - If a specific application programme is necessary for a member of staff's work, then it will be purchased by the school
    - 'Pirate' copies of school owned software for use by other persons either inside or outside the school is an illegal practice
    - Failure to comply will result in disciplinary action

This policy will be reviewed and monitored in line with the school's policy review schedule.

I have read this policy and agree to work in line with Trinity Nursery School's E-Safety policy.

I understand the restrictions of my role in relation to acceptable use of ICT.

NAME (BLOCK CAPITALS) ……

SIGNATURE ……

DATE……