Policy on e-safety and the acceptable use of ICT

ICT has become an integral part of everyday life and when used effectively, can help to enhance the teaching and learning of all pupils. ICT, access to the internet and emerging new technologies are used at St. Teresa's Nursery School to further develop the learning experience. However, the use of these ICT developments also brings risk and this risk is managed by staff, in line with this e-safety policy.

In order to help minimise the risks:

- Children only have access to the internet through adult-led activities.
- Children are encouraged to apply the SMART tips when accessing the internet, see Appendix 1.
- The Principal keeps abreast of e-safety through CEOP (Child Exploitation and Online Protection) and ensures that this information is shared with all staff through relevant training and support.
- Parents and carers receive advice an E-safety Advice Booklet from Nursery and this includes a safety advice checklist for the Under 5s, see Appendix 2.
- All staff have received a copy of this e-safety policy and signed the code of conduct for acceptable use.
- All staff have usernames and passwords which are updated regularly and are not shared with pupils.
- This policy is updated and reviewed in line with the school's policy review schedule.
- This policy is published on the school's website. Important e-safety messages are shared with children as appropriate to their level of understanding, for example through Safer Internet Day.
- The school website only publishes photos of children with prior parental consent.
- Any photos on the school website are nameless and have general caption statements only.

E.S AFETY

ACCEPTABLE USE OF ICT FOR STAFF INCLUDING DATA PROTECTION PROCEDURES

Information Security

Awareness training forms part of induction training and is also shared via the staff handbook, to ensure that all staff are aware of appropriate use of hardware and software in the school and the importance of ensuring that personal data is adequately controlled.

Under no circumstances should a password be divulged to anyone else nor should any employee gain access or attempt to gain access to information stored electronically which is beyond the scope of their authorised access level.

Due care must be taken when transferring data to and from removable media devices such as CDs, USB sticks, PDAs and MP3 players to ensure that personal data is not at risk of either being lost or accessed inappropriately.

When printing personal data, the user must ensure that the material will be sent to a printer in a secure area where the information cannot be inappropriately or inadvertently accessed by other users.

Except to the extent required for the proper performance of duties, staff may not upload, download, use, retain, distribute or disseminate any images, text, materials or software which: -

- are or might be considered to be indecent, obscene or contain profanity;
- are or might be offensive or abusive in that its content is or can be considered to be a personal attack, rude or personally critically, sexist, racist, or generally distasteful;
- encourage or promote activities which make unproductive use of your time;
- encourage or promote activities which would, if conducted, be illegal or unlawful;
- involve activities outside the scope of your responsibilities – for example, unauthorised selling/advertising of goods and services;
- might affect or have the potential to affect the performance of, damage or overload the school's system, network and/or external communications in any way;
- might be defamatory or incur liability on the part of the school or adversely impact on the image of the school.

Electronic Mail and the Internet

Staff must not send or download defamatory, offensive or pornographic e-mail.

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).

E-mail is not 'private' and the school reserves the right to access e-mail and audit the use of the system.

Computer Software

Due to potential virus infection and consequent damage to the business, staff must not load any software into any computer without the prior approval of management. Approval will only be given after virus checking.

Virus protection software is maintained and periodically updated.

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 give rise to disciplinary action being taken, and this could include dismissal.

Monitoring and evaluation
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 St. Teresa's Nursery School's e-safety policy.

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

Name………………………………

Signature………………………….

Date……………

Safety Rules for Children
Appendix 1

S

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

M

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.

A

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.

R

Remember someone online 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!

T

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

Appendix 2

Under 5's checklist

START setting some boundaries now – it's never too early to do things like set limits for the amount of time they can spend on the computer

KEEP devices like your mobile out of reach and make sure you have passwords/PINs set up on them for the times you might lend them to your child... or for when they simply get hold of them themselves!

CHECK the age ratings and descriptions on apps, games, online TV and films before downloading them and allowing your son or daughter to play with or watch them

EXPLAIN your technology rules to grandparents, babysitters and the parents of your child's friends so that they also stick to them when they're looking after your child

REMEMBER that public Wi-Fi (e.g. in cafés) might not have Parental Controls on it – so, if you hand over your iPad to your child while you're having a coffee, they might be able to access more than you bargained for

SET the homepage on your family computer or tablet to an appropriate website like CBeebies

Reference: http://www.vodafone.com/content/parents/get-started.html