**TILERY PRIMARY SCHOOL**

***Together Promoting Success***

E-Safety Policy

![C:\Documents and Settings\TPTracy.Coulthard\Local Settings\Temporary Internet Files\Content.IE5\WROFWR0L\MC900432646[1].png]()

Date agreed: ……………………..

To be reviewed: ………………….

**TILERY E-LEARNING POLICY**

Children are ʻdigital nativesʼ, they have been born into a digital world. Their confidence in using the technologies is high but their awareness of the inherent issues, risks and dangers may be low. They are using technology in new and exciting ways, enhancing and enriching their lives with the many tools on offer, such as web-based technologies that emphasize online collaboration and sharing among users. Young users are no longer passive recipients of online information, but are increasingly creators of digital content, using social software tools to collaborate within a multimedia landscape.

New technologies, new risks

Blocking or banning limits exposure risk in school, however children will continue to experiment online, ever pushing the boundaries. Future employers will be looking for creativity, communication and networking skills. New technologies bring new possibilities and new risks. These risks relate to *content*, *contact* and *conduct*. The purpose of this e-Safety Policy is to empower all those who have a duty of care towards children as well as the children themselves. Equipping children with the skills and knowledge

they need to use technology safely and responsibly when they are online, whether inside or outside school. Education about how to use the technologies safely should be appropriate to the children’s age and level of skill and understanding. However this should not detract from the fun and educational aspects of ICT. Staff are also susceptible to risks so this policy will also identify how they can stay e-Safe and protect the integrity of the whole school community.

The Risks

When considering the use of ICT use at Tilery Primary School it is necessary to consider the age and awareness of the children when delivering a programme of e-Safety education.

Content

There is a risk that children may be exposed to inappropriate content. This maybe material that is pornographic, hateful or violent, encourages activities that are dangerous or illegal, or it is just age inappropriate. Our Internet Service Provider, Northern Grid, filter the Internet content that is accessible in

school. However due to the ever-evolving nature of the internet, this is not foolproof. Children should only use the Internet when they are being supervised by a member of school staff. It is advisable that the sites they visit are also vetted. Through digital literacy education children should also

be taught to become critical and discriminating users of materials they find online and of information

**Tilery Primary School K e e p i n g I T S m a r t**

“Children and young people need to be empowered to keep themselves

safe – this isn’t just about a top-down approach. Children

will be children – pushing boundaries and taking risks. At a public

swimming pool we have gates, put up signs, have lifeguards and

shallow ends, but we also teach children how to swim.”

Dr Tanya Byron

Safer children in a digital world: The report of the Byron Review

provided through ʻdirect contactʼ services, such as email, chat and social networking sites. In the Web 2.0 environment, children are no longer just recipients of content, but are active participants. Through the use of blogs and social networking sites children are able to publish, collaborate and share

information in new ways. Children are able to lie about their age when signing up to such sites, since there is no method of age verification to deter them.

Children and staff should also be made aware of the security risks of accessing certain types of content. These risks include viruses, adware and spyware. They should be taught to always question the reliability and source of any content they access or download. The internet has made it easier to share music, images and texts. Children must be made aware that plagerism and copyright infringement have serious moral, legal and financial consequences.

Contact

A criminal minority makes use of the internet and related services, such as chat rooms, gaming and social software, to make illicit contact with children. This internet contact can progress to other forms of communication such as text messages. These techniques are often referred to as ʻenticementʼ or

ʻgroomingʼ. While online children may also endanger themselves or others by publishing personal information that could enable a stranger to identify and locate them, their family or friends. Cyberbullying is another inappropriate use of new technologies. Bullies are able to torment their victims anonymously at any time of day or night. Children may recieve email, chat or text messages, or be the target of unfavourable websites or social networking groups.

Commerce

There is a financial or commercial risk when using new technologies. Junk email or spam may provide offers that sound too good to be missed, while phishing and similar scams may trick children, parents and staff into revealing personal or financial information which could be used for identity theft.

In addition to this premium-rate services on mobile phones offer ring tones, logos and competitions that may entice children. There is also the risk that children may become obsessed with new technology, neglecting offline

relationships formed through ʻdirect contactʼ. By developing their own judgements of what feels right and what feels wrong, children will be better placed to remain safe when using new technologies.

e-Safety and Special Educational Needs

A pupil with a learning difficulty or disability may be more vulnerable to deceptive messages. For example, many pupils on the autistic spectrum may take messages very literally and could be

persuaded to act upon them. Therefore these vulnerable children may need additional advice on safe

behaviours.

Effective Practice in e-Safety

e-Safety depends on effective practice in each of the following areas:

• Education for responsible ICT use by staff and pupils;

• A comprehensive, agreed and implemented e-Safety Policy;

• Secure, filtered broadband

• A school network that complies with the National Education Network standards and

Specification Writing and reviewing the e-Safety Policy The e-Safety Policy is part of the School Assessment and Development Plan and relates to other

policies including those for ICT, bullying and for child protection.

• The school will appoint an e-Safety Co-ordinator.

• The e-Safety Policy was reviewed in June 2011

• It was approved by the Governors on June 2011

• The next review date is June 2012

Teaching and Learning

Why the internet and digital communications are important

• The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. • internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

• The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

• 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.

• Pupils will be shown how to publish and present information to a wider audience. Pupils will be taught how to evaluate internet content

• The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

• Pupils will be taught the importance of cross-checking information before accepting its accuracy.

• Pupils will be taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access

Information Security System

• School ICT systems security will be reviewed regularly

• Virus protection will be updated regularly

• Security strategies will be discussed with the Local Authority e-Mail

• Pupils may only use their MyDesktop e-mail accounts on the school system

• Pupils must immediately tell a member of staff if they receive offensive e-mail.

• In an e-mail pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission

• Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

• The forwarding of chain letters is not permitted Published content and the school web site

• Staff or pupilʼs personal contact information will not be published. The contact details given online should be the school office.

• The head teacher and ICT Co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupilʼs images and work • Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face

photos of individual children.

• Pupilsʼ full names will not be used anywhere on a school web site or other online space, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.

• Pupil image file names will not refer to the pupil by name

• Parents should be clearly informed of the school policy on image taking and publishing both on school and independent electronic repositories.

Social networking and personal publishing

• The school will control access to social networking sites, and consider how to educate pupils in their safe use.

• Newsgroups will be blocked unless a specific use is approved

• Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

• Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

• Pupils will be advised to use nicknames and avatars when using social networking sites. Managing filtering

• The school will use the Northern Gridʼs filtering service and adhere to itʼs Acceptable Use Policy.

•If staff or pupils come across unsuitable on-line materials, they must click the web browserʼs ʻbackʼ button and report the site to the e-Safety Co-ordinator.

Managing videoconferencing and webcam use

• Videoconferencing should use the educational broadband network to ensure quality of service and security.

•Pupils must ask permission from the supervising member of staff before making or answering a videoconference call.

• Videoconferencing and webcam use will be appropriately supervised for the pupilsʼ age.

Managing emerging technologies

• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

• Mobile phones will not be used during lessons. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

• Staff should not use their own personal mobile phones to take photographs of children.

• Children should not bring mobile phones to school.

• The appropriate use of the Learning Platform (My Desktop) will be discussed as the technology becomes available within the school.

Protecting personal data

• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising internet access

• All staff and Key Stage 2 pupils must read and sign the Acceptable Use Policy before using the internet.

• At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

• Parents will be asked to sign and return a consent form.

• Any person not directly employed by the school will be asked to sign an “Acceptable Useʼ statement before being allowed to access the internet from the school site.

Assessing risks

• The school will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Stockton LA can accept liability for any material

accessed, or any consequence of internet access.

• The school should audit ICT use to establish if the e-Safety policy is adequate and that its implementation is appropriate and effective.

Date of latest update (at least annual):

The school e-safety policy was agreed by governors in: June 2011

The policy is available for staff at: Paper copy given to all staff

The policy is available for parents/carers at: To be uploaded to the school website / available on request

The responsible member of the Senior Leadership Team is: Matthew Davenport

The responsible member of the Governing Body is: Jane Groom

The Designated Child Protection Coordinator is: John Repton

The e-Safety Coordinator is: Matthew Davenport

Has e-safety training been provided for both pupils and staff?

Is there a clear procedure for a response to an incident of concern?

Have e-safety materials from CEOP and Becta been obtained?

Do all staff sign a Code of Conduct for ICT on appointment?

Are all pupils aware of the School‟s e-Safety Rules?

Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?

Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?

Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?

Has an ICT security audit been initiated by SLT, possibly using external expertise?

Is personal data collected, stored and used according to the principles of the Data Protection Act?

Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. Northern Grid, Regional Broadband Consortium, NEN Network)?

Has the school-level filtering been designed to reflect educational objectives and approved by SLT?

This policy was reviewed and amended after consultation with staff and Governors.

Signed: …………………………………...

Date: ……………………

Signed …………………………………. Chair of Governors

Date: ………………………