TILERY PRIMARY SCHOOL

Together Promoting Success

E-Safety Policy

Ratified by

…… Committee Date: October 2017

Signed by Chair of Governors

…….. Date: 21.03.19

To be reviewed:

E-Safety

The internet is now regarded as an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and touch screen tablet devices. Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

Young people have access to the internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care', which applies to everyone working with children.

The school's e-safety policy will operate in conjunction with other policies including those for *Pupil Behaviour, Peer on Peer abuse, Curriculum and General Data Protection Regulation*.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Stockton Community Network including the effective management of NetMedia filtering.
- National Education Network standards and specifications.

Internet Safety – Taken from the PREVENT policy

- The internet provides children and young people with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school block inappropriate content, including extremist content.
- Where staff, students or visitors find unblocked extremist content they must report it immediately to a member of the Senior Leadership Team.
- The e-safety policy refers to preventing radicalisation and related extremist content. Students and staff know how to report internet content that is inappropriate or of concern.

Teaching and learning

Why internet use is important

At Tilery Primary School, we believe that the internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The internet is an essential element of 21st century life for education, business and

social interaction. This school provides pupils with opportunities to use the excellent resources on the internet, along with developing the skills necessary to access, analyse and evaluate them.

- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and is a necessary tool for staff and pupils.
- Pupils use the internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning

- The school's internet access will be designed to enhance and extend education 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.
- The schools will ensure that the copying and subsequent use of internet -derived materials by staff and pupils complies with copyright law.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

E-Safety rules

Responsible Use of the Internet

As part of pupils' computing curriculum Tilery Primary School is providing supervised access to the internet including e-mail.
Our internet access has a built in filtering system that restricts access to sites containing inappropriate content. All our screens are in public view and normally an adult is present to supervise. No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material.

Pupil E-Safety Rules KS2

- I will ask permission before using the internet
- I will use only my own login and password
- I will not access other people's files
- I will not use my own software on the school network
- I will only e-mail people my teacher has approved
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know
- The messages I send will be polite and sensible
- I will not give my name, home address or phone number; or arrange to meet someone unless this is part of an approved school project
- I will not send photos or video of myself or of other pupils unless this is part of an approved school project
- To help protect myself and other pupils, I will tell a member of staff if I see anything I am unhappy with or I receive a message I do not like
- I understand that the school can check my computer files and the internet sites I visit.
- I do not use internet chat rooms
- I will respect copyright and will not copy anyones work and call it my own

Pupil E-Safety Rules KS1 and FS

I will be supervised while on the computer
I will only use the login that I have been given
I will ask permission before going on the internet

Our schools home school agreement which is signed when a pupil starts includes a statement stating their child will follow TPS e-safety rules. The child (age appropriate) signs the home school agreement which states that they will follow the e-safety rules. E-safety rules will be brought to the pupils attention at the start of the first class computer lesson in September and the children's attention drawn to the rules on display. E-safety rules are highlighted and emphasised every January through a whole school initiate and every class has a responsibility to display age appropriate e-safety rules.

Pupils will be taught how to evaluate Internet content

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research internet content. (such as google)
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

It is important to review the security of the whole system from user to internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

Information system security

School ICT systems capacity and security will be reviewed regularly.

- Virus protection will be updated regularly by One IT.
- Personal data sent over the internet or taken off site will be anonymised or password protected.
- Wherever possible staff should save and access documents on a web based portal. If they need to use a memory stick it must be encrypted to store all school related data and password protected.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan. (Can the anti virus scan be automatic)
- Unapproved software should not be uploaded/downloaded.
- Files held on the school's network will be regularly checked. Please refer to our schools GDPR policy.
- The use of user logins and passwords to access the school network will be enforced. All staff and pupils should lock their computers when leaving their workstations.

Share Point

- Pupils/staff will be advised about acceptable conduct and use when using Share Point.
- Only current staff, governors and pupils will have access to the Share Point.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Share Point.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

E-mail

1. KS2 pupils may only use approved e-mail accounts on the school system. (example@sbcschool.org.uk)
2. Pupils must immediately tell a member of staff if they receive any offensive e-mails.
3. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
4. Staff will only use official school provided email accounts to communicate with outside agencies and all other professionals. All communication with parents will be through the generic school email account.
5. The forwarding of chain messages is not permitted.
6. Staff should not use personal email accounts for professional purposes.

Published content and the school web site

- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs or video of pupils are published on the school web site. Please refer to the school entry form.
- Staff may use personal devices such as mobile phones or cameras to take photos or videos of pupils. All images must be deleted from any personal device as soon as possible. If transferred it must be stored in a secure location in line with this school policy.
- Pupils' full names will not be used on social media.

Social networking and personal publishing

- The school firewall will limit access to social media and social networking sites.
- Pupils will use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.
- The schools Facebook page will be closely monitored by members of staff and inappropriate comments will be removed.

Managing filtering

- The school's internet access will include filtering appropriate to the age and maturity of pupils.
- The school will work with One IT and the internet Service Provider to ensure their filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL (website address) will be reported to the School E-Safety Coordinator who will then record the incident and escalate the concern as appropriate.

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.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable IT Use Agreement' (as part of their initial induction) before using any school IT resource.
- On initial induction parents and pupils will be asked to sign and return a form stating that they have read and understood the Acceptable Use document.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- At FS2 and Key Stage 1 access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved on-line materials.
- At Key Stage 2 pupils will be supervised and they will be reminded of the e-safety rules at the start of each lesson which requires them to search the internet. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Stockton LA can accept liability for the material accessed, or any consequences resulting from internet use.
- The school will audit IT provision to establish if the E-safety policy is adequate and that its implementation is effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1998 and breaches will be reported to the Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse will be referred to the headteacher.
- Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure and will need to work in partnership with staff to resolve issues.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's E-Safety ethos.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

- The school will ensure appropriate levels of supervision for students/guests who use the internet and technology whilst on the school site.

Mobile phones and personal devices

- Pupils are not normally permitted to bring mobile phones into school.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Staff are not permitted to use their own personal phones or devices for contacting pupils
- Mobile phones and devices belonging to staff will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used by classroom staff in lesson time unless permission has been given by a member of Senior Leadership Team in emergency circumstances.

Communications Policy

Introducing the E-safety policy to pupils

- E-safety rules are posted in all networked rooms and discussed with pupils at regular intervals.
- Pupils are informed that network and internet use will be monitored.
- E-Safety training programme is embedded in the computing curriculum throughout the school, to raise the awareness and importance of safe and responsible internet use amongst pupils.

Staff and the e-Safety policy

- The reviewed e–Safety Policy will be shared with all staff. All changes will be to the e-safety policy will be shared with relevant members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff are made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff at the start of each school year.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy and E-safety advice in newsletters, the school website/Learning Platform and through school assemblies and parent meetings.

Updated January 2018 – insertion of Teaching & Learning Paragraph 1

Schools e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Head Teacher.

Has the school an e-Safety Policy that complies with LA guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from CEOP, Childnet and UKCCIS etc. been obtained?	Y/N
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers or pupils sign an Acceptable Use Policy?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the General Data Protection Regulation?	Y/N
Is internet access provided by an approved educational internet service provider which complies with DfE requirements?	Y/N
Has the school filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school E-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Officer and/or the E-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the E-Safety Coordinator as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Local Authority into disrepute.

- I will promote E-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the E-Safety Coordinator or the Head Teacher.

- I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

Rules for Responsible Internet Use

The school has installed computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- **I will ask permission before using the internet.**
- **I will use only my own login and password.**
- **I will not access other people's files.**
- **I will not use my own software on the school network.**
- **I will only e-mail people my teacher has approved.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **The messages I send will be polite and sensible.**
- **I will not give my name, home address or phone number; or arrange to meet someone, unless this is part of an approved school project.**
- **I will not send photos or video of myself and other pupils unless this is part of an approved school project.**
- **To help protect other pupils and myself, I will tell a member of staff if I see anything I am unhappy with or I receive a message I do not like.**
- **I understand that the school can check my computer files and the internet sites I visit.**

E-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline www.childline.org.uk

Childnet www.childnet.com

Stockton-on-Tees Local Safeguarding Children Board (SLSCB)
https://www.stockton.gov.uk/children-and-young-people/stockton-on-tees-local-safeguarding-children-board-slscb/

The Children's Hub (Hartlepool and Stockton-on-Tees) childrenshub@hartlepool.gcsx.gov.uk
Telephone 01642 130080

Emergency Duty Team (outside of office hours) Telephone: 01642 524552

Tees LCSB Procedure – www.teescpp.org.uk

ICT Support for Tilery Primary School Help with filtering and network security:
www.oneitss.org.uk Tel: 01642 635570

Internet Watch Foundation (IWF): www.iwf.org.uk

Stockton E–Safety in Schools Guidance www.stockton.gov.uk/children-and-young-people/information-and-training-for-schools-and-childcare-providers/safeguarding-information-for-schools

Stockton Police In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Stockton Police via 01642 326326.
Also visit www.cleveland.police.uk or www.cleveland.police.uk/advice-information/CyberCrime/Internet-Safety.aspx

Think U Know website www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse, www.virtualglobaltaskforce.com

You Tube CEOP - www.youtube.com/user/ceop