Treetops Learning Community

E-Safety Policy Part 2:

The Acceptable Use of the Internet and Related Technologies

December 2021

Treetops Learning Community

E-Safety Policy Part 2:

The Acceptable Use of the Internet and Related Technologies

Document Detail	
Authorised By:	Trustees
Date Approved:	December 2021
Next Review Date:	Ratified by Trustees at the December Board meeting each year

Contents

Section Number	Section Title	Page No.
1	Context	3
2	The Technologies	4
3	Whole School Approach to the Safe Use of ICT	4
4	Roles and Responsibilities	5
5	How Will Complaints Regarding E-Safety Be Handled?	6
Appendix 1	Parental E-Safety Letter and Agreement	7
Appendix 2	Internet Use – Possible Teaching and Learning Activities	10
Appendix 3	Useful Resources for Teachers	11

This Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

1. Context

Harnessing Technology: Transforming learning and children's services [1] sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

The Green Paper *Every Child Matters*[2] and the provisions of the *Children Act 2004*[3], *Working Together to Safeguard Children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

---

[1] http://www.dfes.gov.uk/publications/e-strategy/

[2] See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]

[3] See Every Child Matters website [http://www.everychildmatters.gov.uk]

[4] Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

2. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

3. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A regular e-Safety education programme for pupils and staff.

Reference: Becta - E-safety Developing whole-school policies to support effective practice [5]

[5] http://schools.becta.org.uk/index.php?section=is

4. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the Designated Safeguarding leads within the Senior Leadership Team

Our Designated Safeguarding Leads ensure that they keep up to date with e-Safety issues and guidance through organisations such as The Child Exploitation and Online Protection (CEOP)[6], as well as the DFE.

Designated Safeguarding Leads, with the support of the ICT teacher, will ensure that the e-safety letter and rules (see appendix 1) are sent home annually and parental and pupil agreement is received.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [7] on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

The e-safety rules are clearly displayed in all classrooms to serve as a constant reminder to staff and pupils. The e-safety rules will also be displayed clearly on the school intranet.

The school uses a filtered broadband service via Thurrock Council, however, it is recognised that protection is not guaranteed. Therefore, the IT manager will regularly monitor the network and any issues should be directly referred to the e-safety coordinator who will record all incidents in the 'e-safety log' and take any necessary action.

The IT teacher will teach e-safety lessons on a regular basis (at least termly) to ensure that pupils are empowered in their knowledge of using the internet safely, both at home as well as at school.

Staff are reminded / updated about e-Safety matters at least once a year.

[6] http://www.ceop.gov.uk/

[7] Safety and ICT - available from Becta, the Government agency at:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

5. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by tutor / Head of Key Stage / DSL/ Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to LA / Police.

Key Stage Leaders followed by Designated Safeguarding Leads act as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Appendix 1: Parental e-safety letter, rules and agreement

Dear Parents/ Guardians,

As part of the school curriculum, we can offer pupils supervised access to the internet.

According to the latest guidelines, it is essential that we receive parental permission to allow children access to the internet on an annual basis. We are therefore asking you to read the attached e-safety rules with your child and to then sign and return the permission form as soon as possible as evidence of your approval.

Use of the internet enables pupils to access web sites that are linked to their work in class and is invaluable for supporting their learning in school.

To combat any items that are illegal or potentially offensive to some people, we use a filtered service via Thurrock Council. However we cannot guarantee the success of this filtration so as an additional precaution, you can be assured that children will be supervised by a responsible adult whilst using the Internet.

If you have any problems concerning this matter, please feel free to come into school to discuss this further. Thank you for your cooperation.

Yours sincerely,

Mr Jon Brewer

Head Teacher

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

e-Safety Rules

- We ask permission before using the Internet.
- We only use websites under adult supervision.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people within the intranet.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We only upload video clips to the school intranet.
- Copyright and intellectual property rights must be respected.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Treetops School
e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	***Year Group:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that although the school uses a filtered service, it cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Appendix 2: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Learning Zone The school / cluster VLE
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail Kent Learning Zone Cluster Microsite blogs
Publishing pupils" work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils" full names and other personal information should be omitted. Pupils" work should only be published on „moderated sites" and by the school administrator.	Making the News SuperClubs Plus Headline History Kent Grid for Learning Cluster Microsites National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils" work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives “On-Line” Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 3: Useful resources for teachers

UK Council for Internet Safety – Education for a Connected World – 2020 Edition
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.p

Department for Education – Teaching Online Safety in Schools - 2019
https://www.gov.uk/government/publications/teaching-online-safety-in-schools

Internet Matters.org - Helping parents keep their children safe online
https://www.internetmatters.org/?gclid=EAIaIQobChMIorT-vpXW9AIViaztCh2z1A5WEAAYAiAAEgKCcPD_BwE

NSPCC – Prevention of Cyberbullying
https://learning.nspcc.org.uk/research-resources/schools/stop-speak-support-school-pack

Childnet
https://www.childnet.com/

Becta
https://webarchive.nationalarchives.gov.uk/ukgwa/20110130111510/http:/schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Kidsmart
www.kidsmart.org.uk/

Kent Police – e-Safety
www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html

Think U Know
www.thinkuknow.co.uk/

Appendix 4: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD
http://publications.teachernet.gov.uk
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Kent leaflet for parents: Children, ICT & e-Safety
www.kented.org.uk/ngfl/ict/safety.htm
Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com