Thaxted Primary School

E-safety Policy

Policy Date: Dec 2019	Review Date: Dec 2022	Responsible Person: Headteacher In Cooperation with: Subject Leader for Computing

Thaxted Primary is an inclusive school. We take safeguarding very seriously and all of our policies are developed with a high priority on children's safety and in the light of our safeguarding policy. All of our school policies are interlinked and should be read and informed by all other policies. In particular, the E-safety policy is linked to our child protection, health and safety, photography policy, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHCE.

Rationale

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Information and Communications Technology within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter and a range of other social media
- Mobile/ Smart phones with text, video and web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Aims

Whilst exciting and beneficial both in and out of the context of education, much computing, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).
At Thaxted Primary school, we understand the responsibility to educate our pupils on E-safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

The Role of the Subject leader

As E-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety co-ordinator in this school is the Headteacher who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the E-safety co-ordinator to keep abreast of current issues and guidance through organisations such as, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ E-safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

Teaching and Learning

Computing and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

The school has a framework for teaching internet skills in Computing and PSHE lessons which can be found in the Computing curriculum policy and the E-safety scheme of work.

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button.

Internet Access

The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed internet connectivity.

- Staff will preview any recommended sites, online services, software and apps before use. When searching for images through open search engines pupils are taught about the dangers and educated as to what they should do if they come across anything unsuitable
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

Managing Other Online Technologies and gaming.

Online technologies, including social networking sites if used responsibly, both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking and inappropriate online games websites to pupils within school.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our pupils are asked to report any incidents of Cyberbullying to the school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm.
- Our pupils are advised to comply with Pegi ratings on gaming platforms and also to follow the above guidance when taking part in online gaming where they communicate with other online gamers. Further information regarding game ratings can be found at http://gamesratingauthority.org/GRA/.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting E-safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss E-safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school. Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

Parents/carers are expected to sign a Home School agreement which lists the school's expectations for E-safety. This information is also printed in the front of children's Learning Diaries as follows:

Thaxted Primary School pupils have supervised access to the internet, with filters set up to restrict sites that may not be suitable for children, and we teach them the following rules at an age-appropriate level in line with our 'e-safety' scheme of work:

⇒ I must ask permission before entering any website, unless a teacher has already approved that site;

⇒ I am only to use my login and password, which I will keep secret;

⇒ I must only e-mail or communicate with people I know, or the teacher has approved;

⇒ I make sure that all messages sent will be polite and sensible;

⇒ I must not give my home address of phone number, when sending e-mail or communicating online, nor must I arrange to meet someone;

⇒ I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know;

⇒ I will not use Internet chat except if it is a discussion room that has been set up by the teacher;

⇒ Any work uploaded will be work that I want family and friends to see;

⇒ I will tell a teacher immediately if I see anything I am unhappy with, or I receive messages I do not like;

⇒ I know that the school may check computer files and may monitor the Internet sites that I visit;

⇒ I could be stopped from using the Internet or laptops and ipads if I break any of these rules.

Keeping Safe Online features in our curriculum through PSHE, computing lessons and assemblies throughout the school; further information can found on our school website. The school will take seriously any attempt to misuse the internet or bully others online, whether this be in or out of school. The following website provides advice for ensuring internet safety at home
http://www.thinkuknow.co.uk/

In addition, the school disseminates information to parents relating to E-safety where appropriate in the form of;

- Information evenings
- Practical training sessions e.g. current E-safety issues
- Posters
- School website information
- Newsletter items

E-safety Skills Development for Staff

Our staff receive regular information and training on E-safety and how they can promote the 'Stay Safe' online message. New staff receive information on the school's acceptable use policy as part of their induction. All staff have been made aware of their 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. All staff are encouraged to incorporate E-safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School E-safety Messages

We endeavour to embed E-safety messages across the curriculum whenever the internet and/or related technologies are used. The E-safety policy and advice will promoted widely through school displays, newsletters and class activities.

Children with SEND

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' E-safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-safety. Internet activities are planned and well managed for these children and young people.

Misuse and Infringements procedure

Complaints, concerns and/or issues relating to E-safety in school or at home should be made to the Headteacher. Incidents are logged and action taken to contact parents and address issues of concern in line with our Behaviour policy.

Appendices

Current legislation relating to E-safety follows as an appendix:

Current Legislation

Acts Relating to E-safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on convComputingion, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is

to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convComputinged of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services