Thorpe Primary School

E-safety Policy

At Thorpe Primary School, we are committed to providing a caring, friendly and safe environment for all of our pupils so they can learn in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Thorpe Primary School. We recognise our responsibility to safeguard and promote the welfare of all our pupils by protecting them from physical, sexual or emotional abuse, neglect and bullying.

The subject of Computing 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, at Thorpe, we need to build in the safe and responsible use of digital technologies, in order to arm our children with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe digital environment for Thorpe Primary School.

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-safety Co-ordinator.

- The school's e-safety coordinator is Mr Rob Dawson.
- The e-safety Governor is Gareth Logan
- The e-safety Policy and its implementation shall be reviewed annually.
- Governors are responsible for the approval of the e-safety Policy and for reviewing the effectiveness of the policy.

The role of the e-safety Governor will include:

- Meetings with the e-safety Co-ordinator/Officer.
- Monitoring of e-safety incident logs.

Headteachers and Senior Leaders:

- The Headteacher/Senior Leaders are responsible for ensuring that the e-safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-safety Co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- Provides training and advice for staff.

- Liaises with school Computing technical staff.

- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

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

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.

- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- As part of the new Computing curriculum, all year groups have digital literacy objectives that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.

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

Through computing, we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEND Co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable Use Agreement' before using any digital school resource.

- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher/Senior Leadership Team, by recording the incident in an e-safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-safety Log will be reviewed termly by the e-safety Co-ordinator (See Page 8).

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

- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

E-mail

Currently, the pupils at Thorpe do not have access to e-mail. However, email is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:

- Pupils may only use approved email accounts, if needed, on the school system.

- Pupils must immediately tell a teacher if they receive offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Whole class or group e-mail addresses should be used in school rather than individual addresses.

- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.

- Chain letters, spam, advertising and all other e-mails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended.

Social Networking

- Social networking Internet sites (such as Twitter, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.

- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others.

- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

- All breaches of the e-safety policy need to be recorded in the e-safety reporting book. The details of the user, date and incident should be reported.
- Incidents which may lead to child protection issues need to be passed on to one of the Designated Safeguarding Leaders immediately – it is their responsibility to decide on appropriate action not the class teachers.
- Incidents which are not child protection issues but may require SLT intervention (e.g. cyberbullying) should be reported to SLT on the same day.
- Allegations involving staff should be reported to the Headteachers. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.
- Evidence of incidents must be preserved and retained.
- The curriculum will cover how pupils should report incidents (e.g. trusted adult, Childline)

Mobile Phones

Many mobile phones have access to the Internet and picture and video messaging. They present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils, by permission of the Headteacher, can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are signed in and handed into the school office at 9:00 and collected and signed out at the end of the day.

- The sending of abusive or inappropriate text messages is forbidden.

- Staff should always use the school phone to contact parents.

- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned to silent and stored safely away during the teaching day.

- Staff may use their mobile phones in the staffroom/one of the school offices or the classroom, if no children are in, during their break or lunchtimes.

- Parents cannot use mobile phones on school trips to take pictures of the children.

- On trips, staff mobiles are used for emergency only.

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.

- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.

- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

- The Headteacher or a nominee will inform parent(s)/carer(s) and others present at school events that photographs/videos may be taken on the basis that only photos of their child can be uploaded onto social media.

Staff should always use a school camera to capture images and should not use their personal devices. Photos taken by the school are subject to the GDPR legislation.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.

- Staff and pupils' personal information will not be published.

- The Headteacher, one of the Assistant Headteachers or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Photographs and videos that include pupils will be selected carefully.

- Pupils' full names will not be used in association with photographs.

- Consent from parents will be obtained before photographs of pupils are published on the school Website.

- Work will only be published with the permission of the pupil.

The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School Computing systems capacity and security will be reviewed regularly.

- Virus protection will be installed and updated regularly.

- Security strategies will be discussed with the Local Authority.

- E-safety will be discussed with our Computing support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

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

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature shall be dealt with in accordance with the schools Child Protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during Computing lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School e-safety Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Equal Opportunities

Pupils with additional needs:

- The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.
- Staff are aware that some pupils may require additional 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.

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with the e-safety Coordinator any issue of e-safety that concerns them. This policy will be reviewed annually and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Policy updated October 2018

Incident Log

Thorpe Primary School e-safety Log

Details of ALL e-safety incidents to be recorded by the e-safety Coordinator. This incident log will be monitored termly by the Headteacher, or Member of the SLT.

Date & Time	Name of Pupil or Staff Member	Room and computer/ device number	Details of Incident (including evidence)	Actions and reasons