



Thornborough
Infant School

THORNBOROUGH INFANT SCHOOL

E-Safety Policy

Signed:
Headteacher, Miss. O. Quirke

Signed:
Chair of Governors

Date: October 2020

Review Date: October 2021

In an ever changing technological world, children are accessing the internet at a far earlier age than before. With this in mind, it is never too early to equip children and adults with skills to stay safe online.

This aim of this policy is to ensure the online safety of our students, staff, volunteers and Governing body. It sits alongside our Safeguarding, Anti-bullying and Child Protection policies.

We aim to achieve this by:

Teaching and Learning

We ensure our curriculum enables children to safely enjoy the many learning opportunities and experiences the internet offers. The benefits of using the internet enhances learning and offers a vast amount of information. It also offers educational and cultural exchanges between pupils worldwide. Our children will be taught what acceptable use of the internet looks like and what to do when they are unsure. Under supervision of staff, children will have the opportunity to carefully research topics, and become independent when locating, retrieving and evaluating this research. Children will also have access to age specific resources and activities that will support their learning outcomes. They will also have access to learning whenever and whenever convenient.

Staff will include the use of internet links in their planning and use these resources and links in their teaching and learning. Websites will be evaluated prior to classroom use. In addition, staff will follow the **Teachers Internet Code of Practice**. Staff will also embed a culture of on-line safety within the school through assemblies as well as lessons. Websites such as '**ThinkUKnow**', '**NSPCC**'; text rich environment with posters and advice along with open discussions about use of internet in school and at home.

Home school Learning

No Home/School online learning requires any of our children to access a computer or tablet on their own. Work is practical and curriculum/topic based. The class teacher pre-records a short input, uploads and the children with supervision of their parents can view and complete the tasks.

We use Class Dojo to communicate to the parents and for the parents to upload any activities and tasks the children have completed at home. Once the parents have accepted the link they have access to the messaging service and class stories. Each family only sees their child's portfolio. The class teacher and the Head can view each child's portfolio and marks and comments accordingly.

Each week the parents get a link via Class Dojo to view the weekly learning overview on Padlet. Padlet is an online noticeboard that clearly outlines the objectives in each curriculum area for the week. The noticeboard has links to specific curriculum areas, videos, information and messages from the class teacher and Headteacher. The Padlet link is also uploaded weekly onto the school website.

Equipment/Managing Information Systems

Computers are provided for the school for children and staff to use. They are maintained by staff and IT specialists and regularly checked. Security and Anti-virus (Sophos) of the schools' information system is managed by Bucks County Council. There are appropriate firewalls and restrictions in place to support safer internet use. Children are expected to use equipment sensibly and under adult supervision. When starting school, they (or parents) sign the **Pupils' Internet Code of Practice** and are expected to adhere to this. The search engine used by children is '**Swiggle**'.

Staff are provided with an encrypted memory stick and when using school laptops outside of school, must continue to adhere to the policy. Staff must log out of email or a website when finished and not leave open and/or unattended. Any unusual activity from either a staff or children's PC must be reported to the Headteacher. Staff or children are not allowed to install software onto the PC's.

Digital Images

No images of the children are to be uploaded to the school website or used for any other marketing unless the school has gained written permission from the parents. Names of the children will never be used with

the images. On the occasion that external providers wish to use an image, in addition to the schools consent the Head will contact the parents directly and ask for their permission. Childrens' images will be stored on school equipment, and will be reviewed annually when we have end of year leavers.

Website/Social Media Networking Sites

The local, national and worldwide use of social media has accelerated and used appropriately is a very effective resource for our school marketing and promotion. The Head has a school Facebook account and uses this to promote the learning environment, ethos and philosophy of the school. Passwords and access are secure and limited to the Head. As we are a small rural school this form of social media is also supportive and used in our local community. It allows us and the community to keep up date with important village issues, and acts as a very useful form of communication linking the village.

The school's website is to celebrate the school, children, staff and community. It is also a resource and a means of information for new and existing parents. No images of the children are used unless the school has written parental consent and names of the children are never used. We have a secure web address and passwords to edit and update the website are held by the Head and school Secretary. We regularly have website audits completed by a school governor. We adhere to the statutory information that needs to be provided on a school website and personal information on staff or children is never published.

Given the young age of our children access to social media is blocked. We strongly discourage the use and access to Social networking sites. Pupils are taught never to give out their personal details including locations/friends/family and if they are ever unsure about on line content at home, they must talk to an adult.

Staff and Volunteers must not post any comments on social media that might be deemed derogatory to the school. Staff will adhere to the rule that any new friend request from a child or parent in Thornborough Infant School must not be accepted. Equally no staff should request a new friendship with a current child or parent.

Filtering

The school works with Bucks County Council and 'Turn It On' IT specialists to ensure the security of our systems are protected. If staff or pupils discover unsuitable sites, the URL (web address) will be noted and reported to Bucks County Council.

Internet Access

Children are supervised at all times when accessing the internet. We use the child friendly search engine 'Swiggle'. Parents/Pupils sign the Pupils' Internet Code of practice. Passwords are regularly changed and computers are logged on at the beginning of the day by an adult. Staff also read and sign the Teachers' Internet Code of Practice too. Internet traffic is monitored by Bucks County Council and staff must not access the internet for personal use, including access to Social Media/Networking sites. Staff use of the internet is for professional use only.

Email

Staff are provided with an e-mail account for their professional use and for conducting all school business. Staff know that e-mail sent to an external organisation must be written carefully, and may require authorisation, in the same way as a letter written on the school headed paper. Staff are also made clear that personal e-mail should be conducted through a separate account. Staff are reminded to use 'blind carbon copy' (Bcc) when e-mailing more than one parent contact. Our children do not communicate through email and do not have accounts. Any teaching of email communication will be through the teacher and a safe email account will be set up by Bucks County Council and/or Turn It On for teaching purposes.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation, or GDPR). All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

Mobile Phones

Pupils are not permitted to use mobile phones in school and due to the very young age of our children the likelihood of them having a mobile phone is minimal. Staff are not permitted to use mobile phones during lesson time, but may use them for personal calls outside of lesson time, in a space that no children can or could be present. Staff mobile phones are kept secure in a closed cupboard, set to 'silent'. Staff should not take images of the children on their mobile phones. A school mobile is available for trips. We ask all visitors to turn off their mobile phones on site/and or set to silent and not use in front of children.

Image capturing devices used by parents

Parents are reminded that they must not use their phones to record or take photos of children when we have performances. There will be an opportunity at the end for them to take photos and they are reminded that they must not post an image of their child with another child on social media. Pictures taken are for personal use only.

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 with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones will not be used during lesson time.

Staff/Volunteers

Staff are expected to adhere to this policy and respect its content. This policy and relating policies are readily available and should be read thoroughly and content noted. A copy of this policy is filed and a further copy is accessible on the staff board in the 'Nest'.

Parents

Parents will be guided to the E-Safety policy on the website and in addition through regular Newsletters, emails and other communications. Parents are expected to adhere to this policy and work with the school to create a safe On-Line culture for their children. Parents are kept updated with changes and key events in the calendar – such as E-Safety week, and they are expected to work in collaboration with the school. We strongly recommend parents use parental control software and their child is not left unsupervised using the internet.

Governors

It is the Governors responsibility to read and know this policy and to support the children and staff of Thornborough Infant School to adhere and embed this policy within our school community.

Assessing Risks

Thornborough Infant School will take all 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 Bucks County Council can accept liability for any material accessed or any consequences resulting from internet use.

E-Safety Complaints

Complaints of internet misuse will be dealt with by the Headteacher or the Chair of Governors. Staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with the schools' child protection policy and procedures. Pupils and parents will be informed of the complaints procedure (schools complaint policy) and of the consequences if the internet is misused. All E-Safety complaints and incidents will be recorded by the school – including actions taken.

Appendix 1 – useful resources for Teachers and Parents

BBC Stay Safe

<https://www.bbc.co.uk/newsround/13910067>

Chat Danger

www.chatdanger.com/

Child Exploitation and Online Protection Centre

www.ceop.gov.uk/

Childnet

www.childnet.com

Internet Matters

www.internetmatters.org

Childline

www.childline.org.uk

NSPCC

www.nspcc.org.uk

ThinkUKnow

<https://www.thinkuknow.co.uk/>

Safer Children in the Digital World

www.dfes.gov.uk/byronreview/

Digizen

www.digizen.org/

DfE – Teaching On-line Safety in Schools

www.gov.uk/government/publications/teaching-online-safety-in-schools

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

Internet Safety Zone

www.internetsafetyzone.com

Computer Resources Policy - Student Guidelines

The school has provided computers for use by students. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as floppy disks, CDs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security and Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and floppy disks will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly.

Internet

- Do not access the Internet unless for study or for school authorised / supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/guardian or teacher goes with you. People you contact online are not always who they seem.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.

Pupils' Internet Code of Practice

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any student violates these provisions, access to the Internet will be denied and the student will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

- I will only use the internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher / parents / carer.
- I will never give my password to anyone; even my best friend and I will log off when I have finished using the computer.
- I will never arrange to meet anyone in person without first agreeing it with my parents/teacher/carer and get them to come along to the first meeting.
- I will never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and I will always report it to a teacher or parent.
- I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent.
- I will not look for bad language or distasteful images while I'm online and I will report bad language or distasteful images to a teacher or parent if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I know that my teacher and the Internet service provider will check the sites I have visited!
- I understand that I can access only sites and material relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material.
- I understand that I will not be able to use the Internet if I deliberately hack into the schools' or other systems.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I know that the contents of my e-mail messages will be monitored by the Network Manager
- I may not download software from the Internet (including screen savers, games, video clips, audio clips, *.exe files).
- I know that information on the Internet may not always be reliable and sources may need checking. Web sites may be sponsored by advertisers.
- I will not use e-mail to send or encourage material which is pornographic, illegal, offensive or annoying or invades another person's privacy.

School **Thornborough Infant School** ... Pupil's Name

I have read the Pupils' Code of Practice and I have discussed it with our child. We agree to support the school's policy on the use of the Internet.

Signed Pupil Date
(Parent/Guardian/Carer).

Computer Resources Policy - Teacher Guidelines

The school has provided computers for use by teachers. They offer access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all teachers, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Do not install, attempt to install, or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as floppy disks, CDs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security & Privacy

- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number or your school's name, or send them your picture.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Computer storage areas and floppy disks will be treated like school lockers. Staff may review files and communications to ensure that users are using the system responsibly.

Internet

- Do not access the Internet unless for school activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of ICT staff.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any teacher violates these provisions, access to the Internet will be denied and the teacher will be subject to disciplinary action.

Teachers Internet Code of Practice

- Teachers should be familiar with the school's Network, Internet, e-mail and web site creation policies and the pupils' code of practice for Internet use.
- Teachers should closely monitor and scrutinise what their pupils are accessing on the internet including checking the history of pages.
- Computer monitor screens should be readily visible for the teacher, so they can monitor what the pupils are accessing.
- Pupils should have clear guidelines for the content of e-mail messages, sending and receiving procedures.
- Use of the Internet should be supervised by a teacher or adult.
- Pupils should be taught skills and techniques to enable efficient and effective use of the Internet.
- Pupils should have a clearly defined focus for using the Internet and e-mail.
- If offensive materials are found the monitor should be switched off, any printed materials or disks should be confiscated and offensive URLs should be given to the IT Co-ordinator who will report it to the Internet Service Provider.
- Virus protection has been provided by the school as viruses can be down loaded accidentally from the Internet. Pupils bringing work from home, on floppy disc, could also infect the computer - some viruses will format your hard disc!
- The recommended ISP will check sites visited by schools.
- It is recommended that pupils do not use open forums such as newsgroups or chat rooms.
- Disciplinary action may be taken if the Internet is used inappropriately e.g. for accessing pornographic, racist or offensive material for personal financial gain, gambling, political purposes or advertising.
- Software should not be downloaded from the Internet (including screen savers, games, video clips, audio clips, *.exe files).

I have read the Code of Practice for pupils and teachers and I am familiar with the school's policy on the use of the Internet, e-mail, the creation of web sites and network security.

I agree to abide by these policies and the Teacher's Code of Practice.

Name

Signed

Date