Thornton Primary School E-Safety Policy

Last Revised: April 2016 To Be Revised: March 2018

Readopted by Governing Body: 3rd October 2017

Department for Education

Key Stage 1

Pupils should be taught to:

Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2

Pupils should be taught to:

Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

National Curriculum Computing Programmes of Study

Ofsted Inspection Framework 2012:

Outstanding Behaviour Descriptor

- Pupils are fully aware of different forms of bullying, including cyber-bullying and prejudice-based bullying, and actively try to prevent it from occurring. Bullying and derogatory or aggressive language in all their forms are very rare and dealt with highly effectively.
- All groups of pupils are safe and feel safe in school and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations, including in relation to e-safety.

THORNTON PRIMARY SCHOOL
Since 1930

Ofsted
raising standards
improving lives

The purpose of this policy is to:

- Identify out the key principles expected of all members of the school community at Thornton Primary School in relation to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Thornton Primary School
- Support school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Risks Identified:

Content	• exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse • lifestyle websites, for example pro-anorexia/self-harm/suicide sites • hate sites • content validation: how to check authenticity and accuracy of online content
Contact	• grooming • cyber-bullying in all forms • identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
Conduct	• privacy issues, including disclosure of personal information • digital footprint and online reputation • health and well-being (amount of time spent online (Internet or gaming))

	• sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images) copyright (little care or consideration for intellectual property and ownership – such as music and film)

Responsibilities of the School Community:

Head Teacher (Mrs S.Simmons)	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. BGFL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)
E-Safety Coordinator/ Designated Safeguarding Lead (Mrs S. Simmons/Mr Lee Hodges)	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents • promotes an awareness and commitment to e-safeguarding throughout the school community • ensures that e-safety education is embedded across the curriculum • liaises with school ICT technical staff • To communicate regularly with SLT and Governors to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an e-safety incident log is kept up to date • facilitate training and advice for all staff • liaise with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: · sharing of personal data · access to illegal / inappropriate materials · inappropriate on-line contact with adults / strangers · potential or actual incidents of grooming · cyber-bullying and use of social media
Governors	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

	• To support the school in encouraging parents and the wider community to become engaged in e-safety activities.
Computing Curriculum Leader (Mr Lee Hodges)	• To ensure the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly. • Ensure E Safety Policy is annually reviewed and updated
ICT Network Manager/Policy Central/Network Services (Mr S. Muhammed)	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users only access the school's networks through an authorised and properly enforced password protection policy. (Policy Central) • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) – Enterprise Console-Network Services. • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • BGFL is informed of issues relating to the filtering applied by the Grid • That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • That the use of the network and email is regularly monitored in order that any misuse / attempted misuse can be reported to the *Deputy Head Teacher (Policy Central).* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Office Staff	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All Staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreements in relation to all devices used within the school. • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy. • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of e-safety policies
Parents/Guardians	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to consult with the school if they have any concerns about their children's use of technology
Any Visitor to Thornton Primary School	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Expected Conduct

All Members of the School Community	○ Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. ○ need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences ○ need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so ○ should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school ○ will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
Staff	○ are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils	○ should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
Parents/Guardians	○ should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school ○ should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management at Thornton Primary School:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors.
- Parents / guardians are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Management of in School Systems and Networks:

- Has the educational filtered secure broadband connectivity through the BGFL and so connects to the 'private' National Education Network;
- Uses the BGFL Net Sweeper or equivalent filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of anti-virus software (from BGFL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or BGFL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;

- Has blocked pupil access to music download - except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the BGFL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment, BGFL secure platforms.
- Requires staff to preview websites before use [where not previously viewed or cached] to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the teacher (pupils) or system administrator (staff). Our system administrator(s) logs or escalates as appropriate to the Technical service provider or BGFL/Link2ICT Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup) at Thornton Primary School

- Uses individual, audited log-ins for all users.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Ensures the Systems Administrator / network manager is up-to-date with BGFL services and policies / requires the Technical Support Provider to be up-to-date with BGFL services and policies;
- Storage of all data within the school will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Thornton Primary School:

- Ensures staff read and sign that they have understood the school's e-safety Policy and Acceptable Use Policy documents. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username.
- All pupils have their own unique username and password which gives them access to the Internet;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager/ICT technicians; equipment installed and checked by approved Suppliers / LA electrical engineers
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Makes clear responsibilities for the daily back up of SIMS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);

- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

School Website:

- ○ The Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- ○ Uploading of information is restricted to our website authorisers: Millie Jackson and Michelle Mcall-Hughes;
- ○ The school web site complies with the statutory DfE guidelines for publications;
- ○ Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- ○ The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual e-mail identities will not be published;
- ○ Photographs published on the web do not have full names attached;
- ○ We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- ○ We do not use embedded geodata in respect of stored images
- ○ We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

N.B. Currently the school does not have an online learning platform. If one was introduced this policy would be updated accordingly.

Social networking:

- ○ Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to Thornton Primary School or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

CCTV:

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.

Equipment and Digital Content:

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, pupils' & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupils must not bring mobile phones into school, if a parent or guardian feels that there is a justified need for their child to bring a mobile phone into school this will be discussed with the Head Teacher and if permission is given the mobile phone is to remain switched off in the school safe whilst the school day is in session. Staff members may use their phones during school break times but not in the presence of children. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices:

- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

Staff use of personal devices:

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video:

At Thornton Primary School:

- We gain parental / guardian permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use;

- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal:

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.