Key Stage 2
National Curriculum

Pupils should be taught:

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

THORNTON PRIMARY SCHOOL

E-Safety & Media Policy

September 2020

Ofsted Outstanding grade descriptor

The grade descriptor for outstanding includes:

- Pupils are fully aware of different forms of bullying, including Cyberbullying and actively try to prevent it from occurring. Bullying and derogatory or aggressive language in all their forms are rare and dealt with highly effectively.
- All groups of pupils are safe and feel safe at 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.

Table of Contents

1. Introduction

Thornton Primary School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. 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, at Thornton Primary School we 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.

E-Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for Thornton 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 school's E- Safety Leader is supported by the computing technician is Mr M Sajid

- The E-Safety Governor is Tharack Ahmed
- The E-Safety Policy and its implementation shall be reviewed annually.
- It is approved by the Governors and will be reviewed annually
- It is to be used/read in conjunction with our other Safeguarding Policies:

Appendix
Anti-Bullying Policy
Behaviour Policy
Child Protection Policy
Code of Conduct (Teachers and Support staff)
GDPR Policies
Social Media Policy
Code of Conduct (Teachers and Support staff)

The purpose of this policy is to:

- Identify 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 behavior 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.

2. Risks Identified

The main areas of risk for our school community can be summarised as follows:

Content

- Ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in-app purchases), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites, hate sites, sites inciting radicalisation and /or extremism
- Exposure to inappropriate content, including online pornography
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp and other apps.
- Data breach
- 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)
- Inappropriate messaging or 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)

3. Responsibilities of the School Community

Head Teacher	• 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 Lead	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/ documents • To promote an awareness and commitment to e-safeguarding throughout the school community • To ensure that e-safety education is embedded across the curriculum • To liaise 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 • To facilitate training and advice for all staff
Designated Safeguarding Lead	• To liaise with the Local Authority and relevant agencies • To ensure Governors receiving regular information about e-safety incidents and monitoring reports. • To be 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	• To ensure the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly. • To ensure E Safety Policy is annually reviewed and updated
ICT Network Manager/ Policy Central/ Network Services.	• To report any e-safety related issues that arise 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 • To ensure the school's policy on web filtering is applied and updated on a regular basis • To ensure BGFL is informed of issues relating to the filtering applied by the Grid • To keep 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 • Regularly monitor 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 • Understand the importance of reporting abuse, misuse or access to inappropriate materials • Know what action to take if they or someone they know feels worried or vulnerable when using online technology. • Know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • Know and understand school policy on the taking / use of images and on cyber-bullying. • 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 • 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/Carers	• Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice. • 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 • 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

4. 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 • Know that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
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 sign 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

5. 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 curriculum, all year groups have online safety/PSHE lessons that focus on different elements of staying safe on line. These lessons include topics from how to use a search engine, digital footprints, **STOP** and **THINK** before they **CLICK** and cyberbullying.
- E-Safety Ambassadors are appointed from Years 4, 5 and 6.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Staff preview websites before use, direct students to age/subject appropriate website. Plan the curriculum context for Internet use to match pupil's ability, using child-friendly search engines where more open Internet searching is required; e.g. Watchkin, Ask for kids, Google Safe Search, Swiggle, Kiddle, yahoo for kids.

Through computing we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, 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 SLT & Governor meetings and also with 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.

Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

- Pupils should be helped to understand the need for the student / pupil Acceptable User Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with an unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Pupil e-Safety curriculum

Thornton Primary school has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. We use Purple Mash and Google Internet Legend (Be Internet Legends was designed with support from leading experts in internet safety, including Parent Zone, Internet Matters and CEOP. The programme is also fully accredited by the PSHE Association). This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a website / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- E-Safety Ambassadors will be appointed from Years 4, 5 and 6;
- To know how to narrow down or refine a search;
- To understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post photos or videos of others without their permission;

- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- For year 5/6 pupils to understand why and how some people will 'groom' young people to manipulate, exploit and abuse them (children and young people who are groomed can be sexually abused, exploited or trafficked).
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

We ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop- ups; buying on-line; on-line gaming / gambling;

Vulnerable Learners

Thornton Primary School recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

We will ensure the effective and safe provision of tailored online safety education. We will obtain input and advice from specialist staff as deemed necessary.

6. 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 behavior of users are generally positive and there is rarely need to apply sanctions.

- All members and the 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 contributes 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 and 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.

Reporting

All breaches of the Online Safety policy need to be recorded on CPOM's using the E-safety category, this is then reported to the appropriate staff members. 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 the Head teacher / SLT 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. online bullying) should be reported to SLT on the same day.

Allegations involving staff should be reported to the Headteacher. 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. CEOP button, trusted adult, Childline)

Handling Online Safety Complaints/Incidents

- Complaints of Internet misuse will be dealt with by the Head teacher.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school 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.

Remember:

- Child welfare is of principal concern – the best interests of children take precedence.
- If there is any immediate danger, contact the police on 999.
- Refer to all appropriate agencies.
- Always adhere to local safeguarding procedures and report to the DSL and Headteacher within.

Responding to Complaints

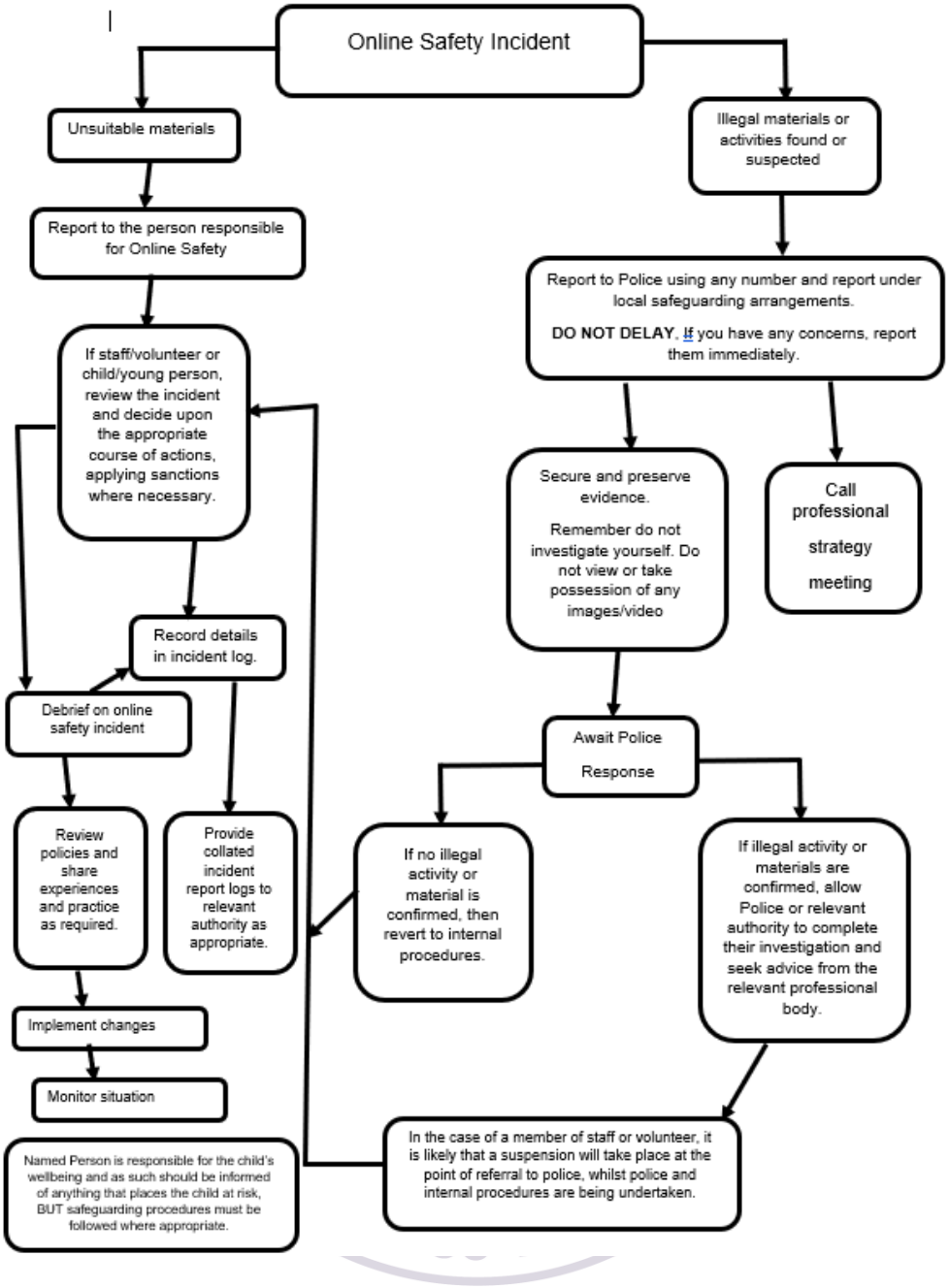
There are a number of sources from which a complaint or allegation might arise, including those from:

- A child or young person
- An adult
- A parent/carer
- A member of the public (including a friend or relative)
- A colleague

There may be up to three components in the consideration of an allegation:

- A police investigation of a possible criminal offence.
- Enquiries and assessment by children's social care or adult social care relating to whether a child, young person or adult at risk needs protection or services.
- Consideration by an employer of disciplinary action in respect of individual (including suspension).

It is also the responsibility of the member of staff to inform their line manager if they are being investigated in relation to children, young people or adults at risk with respect to protection concerns outside of work. They should also report if their own children/stepchildren/children they are living with become subject to child protection matters or an adult related to them or living with them become subject to adult protection matters. The line manager must report this to the DSL and Head Teacher (if DSL is not the Head Teacher).



7. 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. Kiddle for kids and 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.

8. 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.

8.1 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;
- Provide pupils with individual network log-in usernames;
- 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.

9. 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: SLT and Admin team;
- 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.

10. 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

11. 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.

12. 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 Headteacher 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 Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher 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 handheld 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.

13. Students' use of personal devices:

Students are not allowed to bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

14. 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.

15. Photography and Videos

School-owned devices

- Staff are encouraged to take photos and videos of pupils using school equipment; however, they may use other equipment, such as school-owned mobile devices, where the DPO has been consulted and consent has been sought from the Headteacher prior to the activity.
- Where school-owned devices are used, images and videos will be provided to the school at the earliest opportunity, and removed from any other devices.
- Staff will not use their personal mobile phones, or any other personal device, to take images and videos of pupils.
- Photographs and videos taken by staff members on school visits may be used for educational purposes, e.g. on displays or to illustrate the work of the school, where consent has been obtained.
- Digital photographs and videos held on the school's drive are accessible to school staff only. Photographs and videos are stored in labelled files, annotated with the date, and are only identifiable by year group/class number – no names are associated with images and videos. Files are password protected, and only staff members have access to these passwords – these are updated termly to minimise the risk of access by unauthorised individuals.

Use of a professional photographer

If the school decides to use a professional photographer for official school photos and school events, the Headteacher will:

- Provide a clear brief for the photographer about what is considered appropriate, in terms of both content and behaviour.
- Issue the photographer with identification, which must be worn at all times.
- Let pupils and parents know that a photographer will be in attendance, at an event and ensure they have previously provided consent to both the taking and publication of videos or photographs.
- Not allow unsupervised access to pupils or one-to-one photo sessions at events.
- Communicate to the photographer that the material may only be used for the school's own purposes and that permission has not been given to use the photographs for any other purpose.
- Ensure that the photographer will comply with the requirements set out in GDPR.
- Ensure that if another individual, such as a parent or governor, is nominated to be the photographer, they are clear that the images or videos are not used for any other anything other than the purpose indicated by the school.

Permissible photography and videos during school events

If the headteacher permits parents to take photographs or videos during a school event, parents will:

- Remain seated while taking photographs or videos during concerts, performances and other events.
- Minimise the use of flash photography during performances.
- In the case of all school events, make the focus of any photographs or videos their own children.
- Avoid disturbing others in the audience or distracting pupils when taking photographs or recording video.
- Ensure that any images and recordings taken at school events are exclusively for personal use and are not uploaded to the internet, posted on social networking sites or openly shared in other ways.
- Refrain from taking further photographs and/or videos if and when requested to do so by staff.

Storage and retention

- Images obtained by the school will not be kept for longer than necessary.
- Hard copies of photos and video recordings held by the school will be annotated with the date on which they were taken and will be stored in the school office. They will not be used other than for their original purpose, unless permission is sought from the Headteacher and parents of the pupils involved and the DPO has been consulted.
- Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.
- The IT Operations Manager will review stored images and videos on a termly basis to ensure that all unwanted material has been deleted.
- Parents must inform the school in writing where they wish to withdraw or change their consent. If they do so, any related imagery and videos involving their children will be removed from the school drive immediately.
- When a parent withdraws consent, it will not affect the use of any images or videos for which consent had already been obtained. Withdrawal of consent will only affect further processing.
- Where a pupil's security risk has changed, the DSL will inform the Headteacher immediately. If required, any related imagery and videos involving the pupil will be removed from the school drive immediately. Hard copies will be removed by returning to their parents or by shredding, as appropriate.

- Official school photos are held on SIMS alongside other personal information, and are retained for the length of the pupil's attendance at the school, or longer, if necessary, e.g. due to a police investigation.
- Some educational records relating to former pupils of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Monitoring and review

- This policy will be reviewed on an annual basis by the Headteacher and the DPO. The next scheduled review date for this policy is September 2021.
- Any changes to this policy will be communicated to all staff members and, where appropriate, parents.

16. 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.