Policy & Procedure

Thornton
Primary School

Achieving Success
By Working Together

Online Safety Policy 2024

This policy was agreed by the Governing Body on 22nd May 2024 and will be reviewed as required.
Signed: Chair of Governors:
Date: 22nd May 2024

Statutory Policy

The aims of this policy are:

- To keep everyone safe online.
- To help develop a culture of openness about life online and how to stay safe.
- To guide staff, volunteers and governors in how to keep pupils safe online with regards to the curriculum and to internet filtering and monitoring.
- To comply with legislation regarding online safety.

Writing and reviewing the Online Safety Policy at Thornton

- The Online Safety Policy relates to other policies including those for Curriculum, Teaching and Learning, Behaviour, Anti-Bullying, Safeguarding and IT Acceptable Use.
- The Head teacher, senior leadership team and Computing Leader have the overview for Online Safety in the school.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- This policy has been written following the most up to date guidance in Teaching Online Safety in Schools, DfE.

The Computing Leader and DSL/ Head teacher will:

- Take day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents, in partnership with the school's DSL and DDSLs as required;
- Promote an awareness and commitment to online safety throughout the school community;
- Ensure that Online Safety education is embedded across the curriculum
- Liaise with school IT technical staff;
- Communicate regularly with the Governing body to discuss current issues, review incident logs and filtering / change control logs;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident;
- Provide parents guidance about current online issues.
- The DSL is responsible for ensuring the appropriate filtering and the monitoring of this is in place when pupils access the internet in school.

Teaching and learning

Importance of internet and digital communications

Being online is an essential element of life in the 21st century for education, business and social interaction. The school has a duty to deliver Online Safety content across the curriculum, which ensures pupils use the internet and technology in a safe, considered and respectful way, so that they can successfully positively participate in the online world. Pupils will also explore where to go for help and support when they have concerns about content they encounter online.

Being online is a part of the curriculum and a necessary tool for staff and pupils. The benefits of being online in education include:

- Access educational resources to enhance and enrich the taught curriculum

- Support to scaffold learning across the curriculum
- Educational and cultural exchanges world-wide
- Cultural, vocational, social and leisure use in and beyond the school setting
- Engagement in research and expertise in various curriculum areas
- Staff continuous professional development to stay up to date with current educational initiatives and practices
- provide a platform for smarter working practices to reduce workload
- Access to a broad range of professionals to enhance the curriculum, pupil wellbeing and safety

Online Safety Curriculum

- The school will deliver an Online Safety curriculum that is regularly reviewed and updated. This is taught as part of the Computing and PSHE curriculum.
- We also run regular Online Safety assemblies.
- The Online Safety curriculum will reflect current statutory and non-statutory guidance and good practice.
- The school will ensure that Online Safety curriculum is progressive, age-related and scaffolded where necessary, to meet the needs of all pupils.
- Staff will reinforce Online Safety messages in the use of IT across the curriculum.
- Pupils will be taught what being online includes and acceptable practices.
- Pupils will be taught what is not acceptable online and be given clear objectives for online activity.
- Pupils will be educated in applying effective strategies to engaging positively in life online.
- Pupils will be shown how to publish, present and share information appropriately to a wider audience.
- Pupils will be taught how to navigate, manage and evaluate online content, through explicit coverage of Online Safety strands.
- Pupils will be taught to identify potential harms and risks online.
- Pupils will be taught to be critically aware of the materials they read and they will be shown how to validate information before accepting its accuracy.
- Pupils will be taught how and when to report unpleasant online content e.g. older pupils may be taught to use the CEOP Report Abuse icon. All pupils will be taught to report online concerns to a trusted adult without delay.
- Pupils will be taught to recognise techniques used online for persuasion.
- Pupils and staff will be taught / discuss how technology can affect wellbeing.
- Teachers will refer to relevant school documentation and the DfE's 'education for a connected world framework' and 'Project Evolve' to help plan, deliver and resource Online Safety curriculum content.
- Pupils will be taught a 'stop, close, tell' approach.

Communicating and introducing the Online Safety Policy to pupils

- Appropriate elements of the Online Safety Policy will be shared with pupils.
- Pupils will be informed that network and online activity will be monitored.
- Curriculum opportunities to gain awareness of online issues and how best to deal with them will be provided for pupils.

Acceptable Use

Staff and Governors

- Use of school IT systems is governed by IT Acceptable Use Policies, which ensure that all staff and pupils will be safe and responsible online users and of other digital technologies.
- All staff will be expected to sign to say they have read the Online Safety Policy on an annual basis.
- All staff must read and sign the IT Acceptable Use Policy for Staff and Volunteers as part of their induction, before using any school IT resource. This can be found as a separate Policy document.
- Any person not directly employed by the school will only be allowed supervised access to the school's IT systems (other than trainee teachers).
- All volunteers will sign an IT acceptable use policy on induction.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- Failure of staff to comply with the IT Acceptable Use Policy may result in disciplinary action.
- Staff who manage filtering systems or monitor IT use will be supervised by senior leadership and have clear procedures for reporting issues.

Pupils

- Pupils and parents will be asked to sign and return the Pupil Acceptable Use Policy at the start of Y3 as pupils start to use more IT equipment independently.
- Failure of pupils to comply with the Pupil Acceptable Use Policy will be dealt with in accordance with the school's Behaviour Policy.
- Cyber-bullying will be dealt with in accordance with the school's Anti-Bullying Policy.
- Pupils deemed as being 'vulnerable online' will be flagged to the Designated Safeguarding Lead, and tailored provision for using technology will be considered.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the school Online Policy.

IT Systems

Information system security

- School IT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Symphony Learning Trust and reviewed regularly.

Filtering

- The overarching responsibility for filtering systems in school lies with the school's DSL.
- Staff, volunteers and governors understand their duty to keep children safe online using the school's internet.
- Staff and governors are trained annually at a minimum to understand their statutory duties regarding online filtering, how the school keeps children safe online through filtering and also how this is monitored.

- Volunteers are trained when they are inducted.
- Staff, volunteers and governors understand that the internet is continually changing, and that vigilance is key.
- School internet access is provided by Schools Broadband and includes filtering appropriate to the age of pupils.
- The school works in partnership with ICTIT to ensure systems to protect pupils are reviewed and improved.
- The school has 2 levels of filtering in place (a higher level for staff including teaching resources such as You Tube) to protect pupils. All pupil devices and any visitor devices are automatically set to pupil filtering.
- The school will perform regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

Monitoring of filtering

- If staff or pupils come across unsuitable online materials, it must be reported to the Designated Safeguarding Lead, which is investigated immediately and the website blocked.
- Should there be a breach, appropriate action is taken to log the breach on the school's online log, to be actioned by the DSL and IT team.
- Should a pupil be found to be searching for inappropriate materials in school, parents would be informed by the DSL, support and education offered to both parents and the pupil, and a log be made on the child's safeguarding record.
- The DSL and IT team receive a weekly filtering log check and action anything suspicious or concerning with ICTIC. They action this to ensure that such materials can no longer be accessed.
- The school engages in regular external filtering testing using the KCSIE recommended SWGFL Test Filtering.
- The school completes an Internet Filtering and Monitoring Standards for Schools and Colleges Check/ Review on an annual basis to ensure the school meets its statutory duties.
- Governors understand their statutory duty to monitor filtering. The safeguarding governor checks the school's logs on a termly basis and as part of the annual safeguarding audit.
- The school uses WAVE 9 for filtering websites and SENSO for device monitoring.

Accounts

- Staff will be provided with a local network account and an Office 365 account with a linked e-mail address (ending in @thornton.leics.sch.uk).
- Pupils will access the local network via a pupil account.
- Staff and pupils will be provided with additional accounts as determined by the school (e.g. to access online teaching and learning resources).
- Use of all school-related accounts will be in accordance with the IT Acceptable Use Policy.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system (those ending in @thornton.leics.sch.uk).
- Pupils will only have access to e-mail accounts for remote learning if required. These will be restricted and monitored at all times. Pupils will not be able to use their email addresses to send and receive emails, but for log in purposes only.

- Email accounts of pupils may be used on infrequent occasions by teachers and pupils in their class during the teaching of using emails safely. This will be closely supervised and restrictions will be reinstated after use.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

Videoconferencing

- If used, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call and be supervised at all times during a call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Social networking

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
- Pupils must not place personal photos on any social network space without permission.
- Pupils, parents and staff will be advised on the safe use of social network spaces (those appropriate for primary pupils).
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils and parents will be reminded about relevant age restrictions when discussing use of social media.
- The use of social media is not permitted at Thornton and pupils attempting to access this will be in breach of the IT Acceptable use policy.

Devices

- School-managed technology will be used by staff and pupils in accordance with the IT Acceptable Use Policy.
- All school devices will be managed carefully and pupils' use of them will be for solely educational purposes.
- Use of personal devices in school will be in accordance with the IT Acceptable Use Policy (for adults only- pupils do not have access to the internet freely in school).
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity.
- The sending of abusive, offensive or inappropriate material is forbidden.
- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Use of personal data and copyright

Published content and the school website

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The 'contact us' page directs emails to the office email address.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate, appropriate and compliant.

Publishing photographs, images and work

- Photographs that include pupils will be selected carefully and will only include pupils for whom permission has been granted by parents.
- Pupils' full names will not be published on the website, particularly in association with photographs.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Parents are reminded of this at key events where they may take photographs e.g. celebration events and assemblies.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Copyright

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

Online Safety Incidents and Concerns

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Symphony Learning Trust, can accept liability for the material accessed, or any consequences of internet access.
- The school will audit IT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

Addressing potential harms and risks

- The school Online Safety curriculum will address potential risks and harms in three key areas: how to navigate online environments and manage information, how to stay safe online, and pupil wellbeing.
- Curriculum content will be regularly reviewed to reflect the different risks that pupils face and remain up to date with current guidance and good practice.
- Teachers will tailor Online Safety lessons to the needs of their pupils in order to provide the most relevant learning experiences.

Monitoring and Reporting

- Online Safety incidents (including cyber-bullying behaviour) will be reported and monitored in line with school procedures, to the Head teacher/ DSL.

- Online Safety incidents of a child protection nature must be referred to the Designated Safeguarding Lead and dealt with in accordance with school safeguarding procedures.

Handling Online Safety Complaints

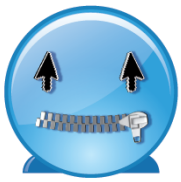
- Complaints of IT misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head teacher. If this complaint is about the Head teacher, then it must be referred to the school's Chair of Governors.
- Complaints of a child protection nature must be referred to the Designated Safeguarding Leader and dealt with in accordance with school child protection procedures.
- Parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the internet.

Enlisting Parents' Support

- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters, and on the school website.
- Parents and carers will from time to time be provided with additional information on current Online Safety issues.
- The school will ask parents to sign the Pupil IT Acceptable Use Policy when the pupil approaches Y3.
- The use of stereotypes will always be challenged.

Appendix 1

Pupil IT Acceptable Use Policy



ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

To keep me safe whenever I use the internet or email, I promise…

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules…

- I understand that the school's behaviour guidelines will be followed

I have read and understand this policy and agree to follow it.

Name of pupil _____

Signed _____ Date _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent/Carer signature _____ Date _____