



THORNTON PRIMARY SCHOOL

Love • Respect • Ambition

ICT, DIGITAL TECHNOLOGY AND ACCEPTABLE USE POLICY

Aims of the Acceptable Use Policy

The purpose of this policy is to ensure that digital technology, the internet and online services are used safely, responsibly and effectively to support teaching, learning and the wider work of Thornton Primary School.

The policy aims to:

- Enable pupils and staff to use the internet, email, Google Classroom and other approved digital services for educational and professional purposes.
- Support learning, research, communication, collaboration, homework and the development of digital literacy.
- Ensure pupils and staff are protected from inappropriate, harmful, illegal or unsafe online content, contact and conduct.
- Promote responsible use of technology, including social media, artificial intelligence (AI), online communication and digital content.
- Protect personal information and ensure that digital technology is used in accordance with the **UK GDPR, Data Protection Act 2018 and current data-protection requirements**.
- Ensure that school filtering and monitoring systems are used appropriately and that online safeguarding concerns are identified, recorded and acted upon.
- Promote good cyber-security practices, including secure passwords, appropriate access to accounts and responsible use of school devices.
- Reinforce the school's Google Classroom and Online Safety expectations.

Thornton Primary School recognises that technology develops rapidly. This policy therefore applies to new and emerging technologies, including generative AI, personal devices, smart technology, online platforms and applications where these are used in connection with school.

Broad Guidelines of the Acceptable Use Policy

Staff

Staff will not:



- Share passwords, login details or authentication information with others, or allow another person to use their account.
- Store, share or disclose personal information about pupils, families or staff unless there is a legitimate school purpose and appropriate authority to do so.
- Use personal contact details, photographs, videos or other information relating to pupils or colleagues inappropriately or without following school procedures and permissions.
- Access, download, upload, store or share material that is illegal, discriminatory, violent, sexually inappropriate, extremist, abusive or otherwise unsuitable for children.
- Use school systems to bully, harass, threaten, intimidate or communicate in a way that could bring the school into disrepute.
- Download, copy or distribute copyrighted material unlawfully or use digital resources without appropriate permission or licensing.
- Use generative AI or other online tools to input confidential, personal or sensitive school information unless specifically authorised and the use complies with data-protection requirements.
- Disable, bypass or attempt to circumvent school filtering, monitoring, security or access controls.
- Use school systems for inappropriate personal, commercial or political activity.

Staff will:

- Use school technology professionally, responsibly and in accordance with safeguarding, data-protection and cyber-security requirements.
- Keep passwords and accounts secure and use appropriate multi-factor authentication where provided.
- Take reasonable steps to protect school devices, data and information from loss, misuse or unauthorised access.
- Ensure pupils are appropriately supervised when using digital technology and provide age-appropriate guidance about online safety.
- Follow the school's filtering and monitoring arrangements and understand that activity on school systems and devices may be monitored for safeguarding, security and operational purposes.
- Report safeguarding, online safety, cyber-security, data-protection or inappropriate-content concerns immediately through the school's established procedures, including reporting safeguarding concerns to the **Designated Safeguarding Lead (DSL)**.
- Ensure pupils understand and follow this policy before, during and after digital-learning activities.
- Use AI and other emerging technologies responsibly, critically and in accordance with school guidance.

The school will maintain appropriate filtering and monitoring systems. These systems will be reviewed at least annually and monitoring incidents will be recorded and acted upon appropriately. Staff understand that filtering and monitoring are safeguarding measures but do not replace effective supervision or professional judgement.

Acceptable Use Policy: Pupils

Pupils will not:



- Use the internet or digital devices without appropriate permission and supervision.
- Use school technology for purposes that are not connected with their learning or authorised school activities.
- Share passwords, usernames or login information.
- Attempt to access another person's account, files or information.
- Give personal information, photographs, videos, passwords or contact details to people online without permission and appropriate safeguards.
- Share personal information, photographs or videos of other pupils or staff without appropriate permission.
- Access, create, download, upload or share material that is inappropriate, harmful, illegal, discriminatory, violent, sexual or extremist.
- Use technology to bully, threaten, harass, upset or deliberately embarrass another person.
- Attempt to bypass school filtering, monitoring or security systems.
- Use generative AI or other online tools inappropriately or present AI-generated work as their own where this has not been authorised by their teacher.
- Install applications, software or extensions without permission.
- Use personal mobile phones, smart watches or other smart technology during the school day except where specifically permitted by the school.

Pupils **will**:

- Follow their teacher's instructions when using digital technology.
- Only access websites, applications, platforms and services that they have been given permission to use.
- Use search engines safely and appropriately.
- Tell a member of staff immediately if they see something online that worries, upsets or concerns them.
- Respect the privacy, files and accounts of other users.
- Use kind, respectful and appropriate language when communicating online.
- Take responsibility for their digital behaviour and understand that online actions can affect others.
- Use technology to support their learning and develop their ability to recognise, manage and report online risks.

Pupils should understand that **the same expectations of behaviour apply online as they do in school.**

Monitoring, Safeguarding and Reporting

Thornton Primary School uses filtering and monitoring systems to help protect pupils and staff from inappropriate and harmful online content. Monitoring may generate alerts or reports which are reviewed in accordance with the school's safeguarding and monitoring procedures.

All users should understand that use of school devices, accounts and networks may be monitored. Monitoring does not replace staff supervision, and staff remain responsible for responding to safeguarding concerns.



Any concern involving online abuse, harmful content, cyberbullying, inappropriate contact, extremist material, exploitation, misuse of technology or a potential data breach must be reported immediately in accordance with school procedures.

The school will maintain appropriate records of significant online safety, filtering, monitoring and cyber-security incidents, including actions taken and outcomes.

Breaches of this Policy

Failure to comply with this policy may result in:

- Temporary or permanent restriction of access to school digital facilities.
- Appropriate behaviour or disciplinary consequences.
- Contact with parents/carers where appropriate.
- Additional safeguarding action where a pupil may be at risk.
- Referral to external agencies or the police where required.
- Further action by the Headteacher and/or Governing Body in accordance with school policies and statutory requirements.

Responses will be proportionate and take account of the individual circumstances, age and needs of the pupil or member of staff, while prioritising the safety and wellbeing of all members of the school community.

Review and Compliance

This policy will be reviewed annually and following significant changes to legislation, statutory guidance, technology or the school's digital provision.

This policy should be read alongside the school's **Safeguarding and Child Protection Policy, Behaviour Policy, Data Protection/Privacy policies, Online Safety arrangements, Cyber-Security procedures and Google Classroom expectations.**

It has been developed with regard to current Department for Education guidance, including **Keeping Children Safe in Education 2026**, DfE filtering and monitoring standards, DfE digital and technology standards, and current data-protection guidance. KCSIE 2026 comes into force on 1 September 2026.

Signed: Mr David Ashcroft, Headteacher

To be agreed by the Finance, Staffing and Resources Committee on 06/10/2026