



Computing policy and code of conduct

Enstone Primary School

Academic year 2026–27

This policy sets out how we teach computing and protect pupils and adults when using technology. It includes acceptable use agreements, incident procedures and separate optional publication permissions. It applies to school systems and equipment on and off site, remote learning, and online conduct that affects the school community.

Status: revised draft for governing body approval. This document sets expectations; it does not certify that technical systems or working practices meet them.

Policy owner: Headteacher.

Curriculum lead: Computing Subject Manager.

Safeguarding lead: Designated Safeguarding Lead (DSL).

1 Purpose and linked policies

We want pupils to understand computing, think logically, create digital content and make safe, informed choices. We retain Purple Mash as our computing scheme from Reception to Year 6, with teaching adapted to our mixed age classes and individual needs.

Staff read this policy alongside the child protection and safeguarding policy, staff code of conduct, behaviour and anti bullying policies, SEND policy and inclusion strategy, data protection policy and privacy notices, photography and video policy, social media policy, health and safety policy, and business continuity arrangements. Staff follow the child protection policy without delay when safeguarding concerns arise.

2 Legal and guidance framework

The policy is informed by the Education Act 2002 safeguarding duties; the statutory computing programme of study; Keeping Children Safe in Education 2026; the current EYFS statutory framework; statutory Relationships Education and Health Education guidance; the Equality Act 2010; the Children and Families Act 2014 and SEND Code of Practice; and the Prevent duty under the Counter Terrorism and Security Act 2015.

Relevant technology legislation includes the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025; the Computer Misuse Act 1990; the Copyright, Designs and Patents Act 1988; the Health and Safety at Work etc. Act 1974; the Electricity at Work Regulations 1989; and the Health and Safety (Display Screen Equipment) Regulations 1992 as amended. The Online Safety Act 2023 principally places duties on regulated service providers; it does not replace the school's safeguarding responsibilities.

DfE digital standards, AI guidance, UKCIS advice and HSE guidance inform implementation. Recommended technical standards are distinguished from statutory duties.

3 Curriculum and learning

Curriculum coverage

Teachers teach computing explicitly and apply it across subjects. The subject manager maps Purple Mash units against statutory requirements and checks that both year groups in each mixed age class receive a coherent sequence without omissions or unnecessary repetition. Cross curricular device use supplements taught computing.

In Key Stage 1 pupils learn how instructions become algorithms and programs, create and debug simple programs, predict what they will do, and create and manage digital content. They recognise everyday uses of technology and learn to protect personal information and ask for help.

In Key Stage 2 pupils design and debug programs, break problems into parts, and use sequence, selection, repetition, variables, inputs and outputs. They reason about errors, understand networks and internet services, evaluate search results, combine software and analyse data. They learn responsible behaviour and different ways to report concerns. The complete statutory programme of study remains the reference for coverage.

Early Years

Reception experiences purposeful, adult supported technology through play, communication, creative work and controllable toys. Unplugged sequencing and problem solving support later learning.

Computing is not a separate EYFS statutory area or early learning goal. Technology complements practical experiences, movement and interaction; it does not displace them.

Teaching and inclusion

Teachers model vocabulary and processes, use practical tasks and discussion, and provide guided practice before independent application. Scaffolds, accessible interfaces, adapted equipment and assistive technology support pupils with SEND or EAL. Reasonable adjustments maintain ambition and enable participation. Online safety teaching takes account of developmental understanding and additional vulnerability, with repeated practice of asking for help.

Teachers plan fair access to devices and resources and provide alternatives for pupils with limited access at home. They select resources that challenge stereotypes and reflect the school community, and avoid fixed assumptions about pupils' capacity to progress.

Assessment and review

Teachers use observation, discussion, debugging tasks and completed work to assess understanding in all three strands: computer science, information technology and digital literacy. Purple Mash assessment tools support professional judgement; platform completion alone is not evidence of secure understanding. Teachers use assessment to plan reteaching and challenge, and include computing outcomes in annual reports to parents.

The Headteacher and subject manager review planning, teaching, pupil work and pupil voice. The governing body receives relevant curriculum and resource reports. Staff development responds to identified needs, new tools and online safety risks.

Online safety education

Teachers coordinate age appropriate online safety teaching across computing, PSHE and Relationships and Health Education. They cover privacy, respectful communication, grooming, bullying, harmful content, scams, commercial pressure and digital wellbeing. Older pupils consider misleading information, manipulated images and AI outputs. Children practise reporting concerns, and teachers reassure them that seeking help is always the right action.

4 Responsibilities and safeguarding

Governing body and Headteacher

Governors oversee curriculum, safeguarding and resources. They designate a governor to oversee filtering and monitoring and receive evidence of effectiveness and improvement actions. The Headteacher assigns operational responsibilities, ensures training, commissions suitable services and checks implementation. The school retains accountability when services are outsourced.

DSL and deputy DSL

The DSL leads online safeguarding, assesses incidents, coordinates support and referrals, and works with IT support on risks. A deputy covers absence. Relevant alerts must reach an available safeguarding lead promptly. Staff use the school's current safeguarding contact arrangements; urgent concerns must not wait for the computing lead or technician.

Computing lead and technical support

The computing lead supports curriculum, resources and staff development. 123ICT is the school's technical support partner and maintains security and technical controls, reports failures and helps investigate incidents within authorised limits. The school uses Securus monitoring software. References to IT support in this policy mean 123ICT working with authorised school staff.

Staff and families

All staff read KCSIE 2026 Part One in full and receive induction, regularly updated safeguarding training and online safety updates, including filtering and monitoring responsibilities. Staff preview resources, supervise pupils, teach safe behaviour and report concerns immediately. Governors receive appropriate safeguarding training. Contractors and volunteers receive guidance proportionate to their access and role.

The school provides parents with the pupil code, clear information about approved learning platforms and how to raise concerns. It explains online risks and the limits of technical controls. Staff address home incidents affecting a pupil's safety or school relationships through safeguarding and behaviour procedures.

Filtering and monitoring

Appropriate filtering and monitoring support supervision and education. Filtering blocks content; monitoring identifies activity and alerts. The Headteacher ensures that the school follows the DfE core standard by assigning leadership, DSL, governor and IT responsibilities, reviewing provision at least annually, blocking harmful material without unnecessary restriction, and maintaining effective monitoring.

The Headteacher, DSL and IT support review coverage of users, devices, locations and off site use, including AI and dynamic content, and record limitations and actions. IT support and the DSL arrange risk based checks, log results and repeat checks after significant changes. IT support maintains appropriate staff and pupil access profiles and a separate controlled network for guests and unmanaged devices. The responsible senior leader approves exceptions, records the reason and obtains the DSL's safeguarding assessment.

The Headteacher ensures that the monitoring plan provides incident reports and immediate escalation of high risk alerts. Named staff and deputies receive and act on them. The school informs users about monitoring, and the Headteacher restricts access to logs to authorised personnel. No system guarantees safety; supervision and reporting remain essential.

Before issuing devices, the Headteacher obtains evidence that controls work as intended. If protection fails or coverage is uncertain, staff stop the affected activity or use a safely supervised alternative while IT support and the DSL assess and remedy the risk.

5 Data protection and secure technology

Personal information and approved services

Staff use personal information lawfully, fairly and transparently, for defined purposes and only to the extent necessary. They keep it accurate and secure and follow the retention schedule. The school explains learning platforms, monitoring, images and relevant sharing in its privacy notices. The DPO advises on lawful bases, special category conditions, rights requests and high risk processing.

Before introducing new apps, cloud services or AI tools, the Headteacher obtains safeguarding, security and data protection checks with the DPO and IT support as appropriate. Checks cover age restrictions, accessibility, advertising, data use and retention, processor contracts, international transfers and children's interests. The Headteacher ensures that the school completes a data protection impact assessment where processing is likely to pose a high risk. Staff must not create pupil accounts contrary to provider terms.

Staff hold school records in approved systems with role based access. They do not use personal email, personal cloud storage or unapproved messaging for school information. They share information securely with authorised recipients and check addresses and permissions. Data protection must not prevent necessary and lawful safeguarding information sharing.

Staff report suspected loss, disclosure or unauthorised access immediately to the Headteacher and DPO. The Headteacher ensures that the school records every personal data breach, with DPO advice. Where notification is required, the school reports to the ICO without undue delay and, where feasible, within 72 hours of awareness. The school informs individuals without undue delay where the breach is likely to create a high risk.

People may raise data protection complaints through the school office or its published electronic route. The school acknowledges these within 30 days, investigates and responds without undue delay. The DPO supports handling and information about escalation to the ICO.

Security and continuity

Users access school systems through individual accounts and strong, unique passwords. IT support implements multi factor authentication in line with the current DfE cyber security standard, limits administrator rights, removes access promptly when roles end, and keeps supported systems, security updates and malware protection current. Users lock screens, log out after use and store portable equipment securely. Only authorised staff install software or change settings.

IT support ensures that devices and any authorised removable storage holding personal information are encrypted. Staff report phishing, suspicious activity, missing devices and ransomware immediately. They follow the agreed cyber incident plan and IT instructions, and avoid further interaction with a suspected compromised system.

The Headteacher ensures that nominated staff maintain asset and licence registers and review replacement needs, energy use and accessibility. IT support securely erases data before reuse, return or disposal, verifies backups, protects a recoverable copy from compromise, and tests restoration. The school does not treat cloud synchronisation alone as proof of a recoverable backup. The Headteacher records recovery priorities and arrangements in the business continuity plan.

Health and safety

Staff position equipment to reduce glare and strain, manage cables and charging safely, and provide breaks and varied activities. The Headteacher ensures that the school completes workstation assessments and provides information and training for staff who are DSE users. Teachers provide suitable posture and accessibility arrangements for pupils.

The Headteacher ensures that the school maintains electrical equipment safely through a risk based inspection and testing regime.

6 AI communications and images

Artificial intelligence

Staff use only tools approved by the Headteacher for school work. Before approval, the Headteacher reviews age limits, safeguarding, data protection, copyright and the DfE AI product safety standards, with specialist advice as needed. Teachers plan and supervise any pupil use to suit their age; pupils do not open independent accounts without approval.

Staff must not put identifiable pupil, family or staff information, confidential records or safeguarding material into unapproved AI tools. Any strictly necessary personal data use in an approved tool requires DPO advice, a lawful basis, appropriate safeguards and transparency. Staff must not allow pupils' original work to train AI models without appropriate copyright permission or a valid legal exception.

Staff check outputs for accuracy, bias, suitability and copyright before use and remain responsible for decisions. Pupils learn that AI can invent convincing information. AI must not replace professional safeguarding judgement or determine significant pupil decisions without meaningful human review. Teachers explain when assistance is permitted; pupils acknowledge it and do not submit generated work as their own. Formal assessments follow the applicable assessment rules.

Communication and remote learning

Staff use approved school accounts and platforms and maintain professional boundaries with pupils and families. They do not contact pupils through personal accounts or accept them as personal social media contacts. The Headteacher approves and records any necessary exception to usual communication arrangements. Staff follow safeguarding procedures for remote teaching, with agreed supervision, appropriate backgrounds and clear reporting routes. They obtain prior authorisation for recording and explain its lawful purpose.

Pupils do not use phones, smart watches or other personal connected devices during the school day unless the school expressly authorises them for a documented educational, medical or accessibility need. Pupils and staff store devices as the school directs. Personal mobile connections can bypass school controls; staff do not provide pupils with personal hotspots. Staff and visitors follow site rules and use authorised school equipment to photograph or record pupils.

Photographs recordings and pupil work

Identifiable images are personal information. The school explains each intended use and its lawful basis. Permission for public or promotional use is separate from curriculum access. Optional choices in Appendix D cover defined purposes and channels; refusal carries no disadvantage. Internal teaching, assessment and records follow the relevant privacy notice and lawful basis rather than blanket publicity consent.

Before publication, staff check the permission record, safeguarding restrictions and the child's wishes. They avoid linking public images to full names or identifying details and check captions and location information. Omitting a name does not guarantee that a child is unidentifiable. Staff store images securely with restricted access and delete them in accordance with the retention schedule.

The school seeks permission separately for new purposes or channels. Where consent is the lawful basis, parents or carers can withdraw it as easily as they gave it. Withdrawal affects future use. Staff remove controlled online copies where practicable and explain that printed copies already distributed and third party copies may not be recoverable.

Parents and visitors follow event photography rules and do not share images of other children publicly without appropriate permission. This is a school safeguarding expectation; personal household photography is not automatically prohibited by data protection law. Anyone with concerns about published images should report them to the school office.

7 Responding to concerns

Immediate response for all staff

- Protect and reassure the pupil. Stop the activity and move the child away from harmful content. Listen without blame; do not promise secrecy.
- Tell the DSL or deputy immediately about safeguarding concerns. If neither is available, follow the safeguarding policy and seek urgent advice or referral directly when needed. Call 999 if there is immediate danger.
- Record facts, the child's own words, time, device and relevant context in the approved safeguarding system. Do not repeatedly question the child or conduct your own investigation.
- Notify IT support about technical failures through the agreed route. The DSL decides safeguarding referrals and safe parent communication; IT support does not decide whether a concern needs safeguarding action.
- Arrange support, address any control failure and review learning or supervision needs. Record actions and outcomes.

Accidental and deliberate access

Accidental exposure is not misconduct. Praise reporting, support the child and assess the filtering failure. Deliberate searching may also indicate distress, abuse or unmet needs; refer to the DSL as appropriate and assess context before a behaviour response. Avoid automatic loss of access. Any restriction must be proportionate, time limited, reviewed and accompanied by access to learning and reasonable adjustments.

Sexual imagery and other harmful content

Do not seek to view, copy, print, save or forward nude or semi nude images of children, including suspected AI generated imagery. Do not ask a pupil to send or download them, and do not direct the pupil to delete evidence. Report immediately to the DSL, who follows UKCIS guidance and consults police or children's social care as needed. Preserve the device safely under authorised instructions. Only the DSL may consider the exceptional circumstances for viewing described in the guidance; staff do not make that decision independently.

For other harmful content, preserve relevant information only through authorised safe procedures. Never revisit suspected illegal material to collect evidence. Cyberbullying, grooming, exploitation, extremism, self harm content and threats follow safeguarding procedures alongside appropriate behaviour support.

Concerns involving adults

Report allegations or concerns about staff, volunteers or contractors to the Headteacher under the safeguarding and staff conduct procedures, including low level concerns. Concerns about the Headteacher go to the Chair of Governors. Do not investigate independently. Use the whistleblowing route if normal reporting is unsafe or ineffective.

Monitoring and review

The Headteacher reviews implementation at least annually, with the subject manager, DSL, DPO and IT provider as relevant. Governors receive assurance on curriculum, training, incidents and controls without unnecessary personal details. Significant incidents and changes prompt earlier review. Following approval, the Headteacher ensures that staff complete the implementation checklist.

Appendix A Adult acceptable use agreement

For staff, governors, volunteers and contractors with access to school systems. This agreement applies on and off site, including remote working. It supports the staff code of conduct and does not replace safeguarding responsibilities.

- I use authorised accounts, devices and services for my role and access only information I am entitled to use. I do not share passwords or allow family members or others to use my school account or equipment.
- I keep school information in approved systems, check recipients before sharing, lock my screen and use required security controls. I report suspected breaches, phishing, loss or compromise immediately.
- I do not disable filtering, monitoring or security controls, install unapproved software, use unauthorised removable storage or try to gain access to another person's files.
- I communicate professionally through school channels. I do not use personal accounts to contact pupils, and I respect confidentiality when using social media.
- I supervise pupils, preview resources and report harmful content, contact or conduct promptly to the DSL. I follow the incident procedure and do not copy suspected illegal imagery.
- I use school approved arrangements for images and recordings, checking permissions and safeguarding restrictions before publication.
- I use AI only as approved, protect confidential and personal information, check outputs and comply with copyright and assessment rules.
- I respect software licences and copyright. Acknowledgement alone does not grant permission; I use content under a licence, permission or applicable legal exception.
- I care for equipment, report damage and return equipment and information when required. School equipment is for authorised professional use; any incidental personal use must be permitted by the Headteacher and comply with these rules.
- I understand that school systems and devices are monitored for legitimate safeguarding and security purposes as explained in privacy notices. Monitoring is proportionate, access is restricted and records follow retention rules.
- I understand that breaches are considered fairly under the relevant conduct, disciplinary or contractual procedures and may require external referral.

Name: _____ Role: _____

Signature: _____ Date: _____

Appendix B Pupil codes of conduct

Younger pupils

- I use technology when my teacher says I can and follow instructions.
- I use my own login. I keep my password private, except when a trusted adult helps me.
- I am kind in messages and respect other people's work.
- I ask an adult before sharing information, taking a photo or sending anything.
- If something worries or upsets me, I stop and tell my teacher or another trusted adult straight away.
- I do not meet someone I only know online.
- I look after equipment and finish safely as my teacher shows me.

Older pupils

- I use only approved websites, apps and tools, with permission. I do not bypass safety controls or use someone else's account.
- I protect personal details, photos, passwords and location information belonging to me or others. I check with my teacher before sharing, downloading, signing up or making a purchase.
- I treat people respectfully. I do not bully, threaten, impersonate or share hurtful content, even as a joke.
- I ask permission before photographing, recording or sharing someone's work. I respect copyright and say where information comes from.
- I check information against reliable sources. Search results, pictures and AI answers can be wrong or misleading.
- I use AI only when my teacher allows it, explain any help I have used and do not claim generated work as my own.
- I do not arrange to meet someone I only know online. If someone asks for personal information, images or a secret conversation, I tell a trusted adult.
- If I see harmful material or receive a worrying message, I stop and tell an adult. I do not reply, forward it or try to investigate.
- I report problems even if I made a mistake. If the first adult cannot help, I tell another trusted adult.
- I look after equipment, save work as instructed and log out when finished. I understand that school devices and accounts are monitored to help keep us safe.

Teachers explain the appropriate code using examples and accessible language. Adults help younger pupils or those who need support; signing is not a test of reading ability. Children are never blamed for reporting a concern.

Appendix C Pupil and parent agreement

Dear Parent or Carer,

Our pupils use technology to create, solve problems and learn about the world. We teach online safety and supervise its use. Filtering and monitoring help us identify risks, but no system is completely effective. Please discuss the appropriate pupil code with your child and return this acknowledgement.

Tell your child to stop and speak to a trusted adult if anything online worries them. Please let the school know about incidents at home that may affect their safety, wellbeing or relationships in school. Use the school office to raise concerns; urgent concerns need direct contact with an available safeguarding lead or emergency services as appropriate.

This is an acceptable use agreement. It is not consent for publicity, data processing generally or independent AI accounts. The school's responsibilities to provide education, make reasonable adjustments and safeguard children apply regardless of whether a form is signed.

Pupil acknowledgement

An adult has explained the code to me. I will try to follow it and ask for help when I need it.

Pupil name: _____ Class: _____

Pupil signature or supported acknowledgement: _____

Date: _____

Parent or carer acknowledgement

I have discussed the code with my child in a way they can understand. I know the school uses filtering and monitoring and that further information is in its privacy notices. I understand that concerns will be addressed through support, safeguarding and proportionate behaviour procedures. Any temporary restriction will be reviewed and alternative access to learning considered.

Parent or carer name: _____

Signature: _____ Date: _____

Please return to the school office. Ask the school if you need an accessible version, help understanding the agreement or details of approved learning platforms.

Appendix D Optional publication permission

Permission is optional. A “No” or blank response means no permission for that listed purpose. Your child will still participate in learning. Images include photographs and video. Internal educational records are managed separately under the school’s published lawful bases.

Pupil name: _____ Class: _____

Photographs or video in printed school promotional publications, such as a prospectus or newsletter.
YES / NO

Photographs or video on the public school website to share school activities and achievements. YES / NO

Examples of my child’s original work in printed school publications. YES / NO

Examples of my child’s original work on the public school website. YES / NO

Circle one answer for each purpose. These choices cover only the channels listed. Social media, press, external organisations and AI model training are not included; specific permission must be considered separately.

Publication permission for pupil work grants permission for these uses only and does not transfer copyright ownership. We will consider your child’s wishes before using their image or work. Images will not be linked publicly with their full name or other identifying details. A photograph may still identify a child to people who know them.

These permissions remain in place while your child attends Enstone Primary School, unless changed. The school checks suitability before each use. Images and work already published are retained or removed in accordance with the image privacy information and retention schedule; consent does not authorise indefinite storage.

You may change or withdraw permission at any time by contacting the school office at office.2103@enstone.oxon.sch.uk or 01608 677268. Withdrawal stops future use for the relevant purpose. The school will remove material from channels it controls where practicable; printed copies already circulated and third party copies may not be recoverable. Withdrawal does not make earlier lawful use unlawful.

Parent or carer name: _____

Signature: _____ Date: _____

Office use: recorded by _____ Date _____

Appendix E Implementation checklist

For the Headteacher and responsible governor before approval and at review. Complete using evidence from school systems and current contracts. These items are operational checks, not findings that the school is non compliant.

Safeguarding roles

Check: Confirm DSL and deputy cover, named governor, alert recipients and urgent reporting routes.

Owner and evidence: _____ Completed: _____

Filtering and monitoring

Check: Confirm the actual filtering provider separately from Securus monitoring, device coverage, off site protection, logs, annual review and weekly reports.

Owner and evidence: _____ Completed: _____

Technical support

Check: Review the 123ICT support contract and escalation contacts; ensure staff know how to report faults and urgent technical concerns.

Owner and evidence: _____ Completed: _____

Cyber security

Check: Obtain evidence of MFA, supported software, updates, access removal, encryption and tested recovery arrangements.

Owner and evidence: _____ Completed: _____

Backups

Check: Verify recoverable backups for curriculum and administration systems; do not rely on assumed Google Drive or OneDrive synchronisation.

Owner and evidence: _____ Completed: _____

Data protection

Check: Check DPO contact information, privacy notices, processor contracts, retention schedule, breach reporting and the electronic complaint route.

Owner and evidence: _____ Completed: _____

AI and platforms

Check: Record approved tools, age restrictions, safeguarding checks, data protection decisions and pupil account arrangements.

Owner and evidence: _____ Completed: _____

Images and pupil work

Check: Align Appendix D with the school image policy, actual channels and retention periods; review existing consents and safeguarding restrictions.

Owner and evidence: _____ Completed: _____

Curriculum and training

Check: Check mixed age coverage, assessment, accessible pupil teaching and staff understanding of incident reporting.

Owner and evidence: _____ Completed: _____

Approval and rollout

Check: Record governor approval, review date and responsible officers; circulate agreements and replace old web links and posters.

Owner and evidence: _____ Completed: _____

Appendix F Sources and review notes

Keeping Children Safe in Education 2026

<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

Computing programmes of study

<https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study>

DfE filtering and monitoring core standard updated September 2026

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>

DfE cyber security core standard

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard>

DfE generative AI in education

<https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education>

UKCIS sharing nudes and semi nudes guidance

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>

ICO Data Use and Access Act changes

<https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/>

ICO photographs in schools

<https://ico.org.uk/for-the-public/schools/photos/>

HSE portable appliance testing

<https://www.hse.gov.uk/electricity/faq-portable-appliance-testing.htm>

HSE display screen equipment

<https://www.hse.gov.uk/msd/dse/>

UK legislation

<https://www.legislation.gov.uk/>

Date Adopted: November 2026

Review Date: November 2027

Signature of Chair of Governors:



Signature of Headteacher:

