ONLINE SAFETY POLICY

Holy Trinity and St John's Church of England Primary School

Vision

Rooted in the love of Christ, we nurture every child to flourish with courage, compassion and community -
becoming a light for others in the world.

Effective from: September 2026

Review date: September 2027

Policy leads: Headteacher, DSL and Online Safety Lead

Approved by: Governing Body

1. Our Vision and Aims

At Holy Trinity and St John's Church of England Primary School, our use of technology is rooted in our Christian vision and values. Technology should help children and adults to flourish, extend learning and strengthen communication. We use it with courage, compassion and responsibility so that every member of our community is respected, protected and able to seek help.

Online safety is an essential part of safeguarding. This policy explains how the school educates pupils, supports families, manages technology and responds to concerns. It applies to pupils, staff, governors, volunteers, contractors and visitors whenever school technology, networks or accounts are used, and to online behaviour away from school where it affects the safety, wellbeing or education of members of the school community.

This Online Safety Policy must be read and actioned in conjunction with the school's whole-school Safeguarding and Child Protection Policy.

Our aims are to build pupils' knowledge and resilience, reduce foreseeable risks, maintain secure and proportionate systems, and make sure concerns are recognised, reported and acted upon without delay. Online safety is a shared responsibility and is treated as a continuous theme across safeguarding, curriculum, behaviour, data protection and staff conduct.

2. Policy Framework and Scope

This policy reflects Keeping Children Safe in Education 2026, the statutory guidance for Relationships Education and Health Education applying from September 2026, the National Curriculum for Computing, the DfE standards for filtering and monitoring and digital technology, and guidance on teaching online safety, mobile phones, searching and confiscation, bullying and preventing radicalisation.

It also has regard to relevant legislation, including the Education Acts, the Education and Inspections Act 2006, the Children's Wellbeing and Schools Act 2026, the Equality Act 2010, the Data Protection Act 2018 and UK GDPR, the Counter-Terrorism and Security Act 2015 and the Human Rights Act 1998. The Online Safety Act 2023 regulates online services; it does not replace the school's safeguarding duties or the need for education, supervision and effective reporting.

The policy covers school-owned and personal devices, school networks and internet access, email, cloud services, websites, learning platforms, social media, messaging, cameras, video and audio, games, wearable or smart technology, and generative artificial intelligence. It should be read with the school's acceptable-use agreements and related safeguarding, behaviour, data-protection, mobile-phone, social-media, image-use, AI and cyber-security arrangements.

3. Understanding Online Risk

The school plans its education and safeguards around four connected categories of online risk. These risks can occur on school systems or elsewhere, and may overlap with abuse or harm taking place face to face.

Risk	What this includes
Content	Illegal, inappropriate or harmful material, including pornography, racism, antisemitism, misogyny, self-harm, suicide, violence, extremism, harmful challenges, misinformation, disinformation, conspiracy theories and AI-generated material.
Contact	Harmful interaction with other users or systems that simulate human contact, including bullying, peer pressure, grooming, exploitation, coercion, scams, unwanted contact and adults or children misrepresenting who they are.
Conduct	Behaviour that causes or increases harm, including harassment, abusive messages, impersonation, sharing personal information, and creating, requesting, sending or forwarding nude, semi-nude, sexualised or humiliating images, including deepfakes and AI-altered material.
Commerce	Online gambling, inappropriate advertising, subscriptions, in-game purchases, phishing, fraud, financial scams, sextortion and other attempts to obtain money, information or images.

4. Roles and Responsibilities

The Governing Body: has overall responsibility for oversight of online safety and for holding the Headteacher to account. Governors ensure that online safety is integrated across safeguarding arrangements, pupils are taught how to keep themselves and others safe, staff receive suitable training, and appropriate filtering and monitoring are in place. The Governing Body receives regular assurance about incidents, trends, training and the annual review of filtering and monitoring.

The Headteacher: ensures that this policy is understood and implemented consistently, responsibilities are assigned, sufficient time and resources are available, and arrangements remain effective when key staff are absent. The Headteacher authorises any exceptional departure from the school's mobile-phone or filtering arrangements and leads the response where staff conduct is involved.

The Designated Safeguarding Lead: holds lead responsibility for online safeguarding. The DSL understands the school's filtering and monitoring systems, responds to alerts and safeguarding reports, maintains appropriate records on CPOMS, works with IT support and the Online Safety Lead, makes referrals where necessary and reports themes and assurance to senior leaders and governors. Online incidents are managed under the child protection and safeguarding policy whenever a child may be at risk.

The Online Safety Lead: coordinates the curriculum and wider online-safety programme, supports staff, pupils and families, monitors emerging risks and patterns, contributes to the annual risk assessment and policy review, and works with the DSL, SENCO, curriculum leaders and technical support. The Online Safety Lead does not replace the DSL's safeguarding authority.

IT support and service providers: maintain secure systems, apply agreed filtering and monitoring controls, protect against malware and unauthorised access, test and update technical safeguards, preserve logs and report failures or alerts promptly. Technical staff act only within their authority and do not make safeguarding decisions in place of the DSL.

All staff, governors, volunteers and contractors: must understand and follow this policy and the applicable acceptable-use agreement, model safe and professional behaviour, supervise pupils appropriately, report concerns and system failures promptly, and never assume that filtering makes an activity safe. Staff maintain professional curiosity where a child may be unable or unwilling to explain an online concern.

Pupils: are taught to use technology safely, respectfully and responsibly, follow the pupil acceptable-use agreement, protect personal information, report anything worrying and seek help from a trusted adult. A pupil who asks for help will be supported and will not be blamed for an abusive experience.

Parents and carers: are asked to reinforce safe use at home, discuss online experiences with their child, support the pupil acceptable-use agreement and tell the school promptly about concerns that may affect a child or the school community.

Visitors and community users: must follow school instructions and the relevant acceptable-use terms when accessing school systems, devices or internet services.

5. Education for Pupils

Online safety is taught progressively from Reception to Year 6 through Computing, Relationships and Health Education, PSHE and relevant learning across the curriculum. Kapow Primary provides the core PSHE and RSHE content that reinforces online relationships, respectful behaviour, wellbeing, privacy and help-seeking. Teachers adapt and supplement these materials to meet statutory outcomes, pupils' needs, emerging risks and the school's Christian vision.

Teaching begins before and alongside access to online services. In age-appropriate ways, pupils learn how to use technology safely and respectfully, keep personal information private, recognise acceptable and unacceptable behaviour, evaluate information and images, resist pressure, protect accounts and devices, and report concerns about content or contact. By the end of primary school, pupils understand that people may behave differently or pretend to be someone else online; information and images can be copied and may be impossible to remove; platforms have age restrictions; privacy and location settings matter; and trusted adults can help.

The curriculum also addresses online bullying, grooming, exploitation, radicalisation, scams, persuasive design, advertising, misinformation, harmful content, image-based abuse, artificial intelligence, chatbots, deepfakes and the creation or sharing of sexualised images. Pupils are taught not to view, copy or forward harmful material and to report it. Practical cyber-security learning includes strong passwords, phishing and social engineering, device security, removable media, multi-factor authentication where relevant, and how to report a cyber incident or personal-data concern.

Lessons use clear ground rules and safe distancing techniques. Staff do not ask pupils to disclose personal experiences publicly. Where content could affect a known pupil, the DSL and teacher consider timing, adaptation and support. External visitors may enhance learning but do not replace planned teaching; their suitability, materials and safeguarding arrangements are checked in advance, and a member of staff remains present.

6. Vulnerability, Inclusion and Equality

Any child can be vulnerable online, and vulnerability can change with age, development and circumstances. Pupils with SEND, communication needs or limited understanding of risk; children in care or previously in care; children experiencing abuse, poor mental health, isolation or family difficulty; and pupils who are, or are perceived to be, different may face increased risks or barriers to seeking help.

Teaching, supervision, reporting routes and technical safeguards are therefore adapted where needed. Staff consider language, cognition, sensory needs, prior experiences and the possibility that a child may not recognise grooming, coercion, exploitation or abuse. Adaptation does not remove a pupil's entitlement to protective knowledge. Online incidents involving prejudice, misogyny, sexual harassment or other discriminatory behaviour are addressed through safeguarding, behaviour and equality procedures.

7. Filtering and Monitoring

The school uses filtering to block harmful and inappropriate content and monitoring to identify activity that may require review. These systems apply to school networks and school-managed devices as configured by the school. They support, but never replace, effective teaching, supervision, professional curiosity and clear reporting routes.

The DSL takes lead responsibility for understanding the systems and safeguarding processes. The Headteacher, DSL, Online Safety Lead and IT support work together to assign operational responsibilities, determine what is blocked or monitored, respond to alerts and maintain records. Access to monitoring information is restricted to authorised people and used lawfully, transparently, necessarily and proportionately.

- Senior leaders review the effectiveness of filtering and monitoring at least once each academic year and after a significant incident, system change or identified weakness.
- The review considers the school's safeguarding risk profile, the needs of pupils including those with SEND, devices and services in use, roles, alert handling, testing, staff understanding and any unreasonable impact on teaching and learning.
- Staff report harmful content that is accessible, educational content that is wrongly blocked, monitoring alerts, suspected bypassing and any failure of a control through the agreed IT route and to the DSL where safeguarding may be involved.
- No user may disable, evade or test a safeguard without explicit authority. Any temporary bypass for a legitimate educational or technical purpose must be authorised, time-limited, supervised and recorded.

Users are informed that activity on school networks, accounts, devices and communication services may be logged or monitored. The school follows data-protection and employment requirements and does not use monitoring indiscriminately.

8. Acceptable Use, Accounts and Devices

The school's current acceptable-use agreements form part of this policy framework. Staff, governors and authorised users agree to the Staff and Governor Acceptable Use of Technology Policy. Pupils and parents or carers agree to the age-appropriate pupil agreement. Relevant visitors are informed of the terms that apply to them.

Users must access only the accounts, systems and information authorised for their role; protect passwords and authentication details; lock unattended devices; use approved storage and communication systems; respect copyright; and report loss, theft, phishing, malware, unauthorised access or accidental disclosure promptly. School information must not be moved routinely to personal email, cloud storage, messaging apps, USB media or other unapproved services.

School devices remain school property. Staff using them away from school must keep them password-protected, encrypted where provided, updated and physically secure; prevent access by family or friends; avoid exposing confidential information in public places; and contact the designated IT route immediately if security is in doubt. Personal devices may be used for school business only where a documented school arrangement permits it.

9. Mobile Phones and Smart Technology

The school is a mobile-phone-free environment for pupils throughout the school day, including lessons, transitions, breaktimes and lunchtimes. This includes smart watches and other technology with similar communication or recording functions. Any exception, for example a specific medical, accessibility or safeguarding need, must be documented and authorised by the Headteacher. Where a device is brought to school under local arrangements, it must be switched off and stored as directed.

Staff use of phones and connected devices must not interfere with teaching, supervision, safeguarding or professional duties. Personal devices must not be used to photograph or record pupils, access or store pupil information, record confidential meetings or communicate with pupils through personal accounts unless an exceptional, documented procedure has been expressly authorised. School images and recordings are created only for a legitimate purpose using approved arrangements.

10. Artificial Intelligence and Emerging Technology

Artificial intelligence may support education and school work when its use is approved, age-appropriate and consistent with the school's AI policy. It does not replace professional judgement or safeguarding decisions. New tools and new uses are risk-assessed before adoption, including their age requirements, privacy, data use, filtering, content safeguards, bias, accuracy and impact on pupils.

Identifiable or confidential pupil, safeguarding, medical, SEND, assessment, behaviour, staff, image or audio data must not be entered into an AI tool unless the school has expressly approved that system and use following appropriate data-protection assessment. Outputs must be checked for accuracy, bias, harmful content, copyright and suitability before use.

The school treats AI-enabled bullying, impersonation, deepfakes, deep nudes, fabricated audio or video and sexualised or humiliating content as serious safeguarding and behaviour concerns. Pupils are taught that apparently human chatbots may create false intimacy, provide harmful advice or

encourage unsafe disclosure. Suspected misuse is reported immediately to the DSL and handled under the child protection, behaviour and AI policies.

11. Online Bullying, Harmful Sexual Behaviour and Image Incidents

Online bullying includes repeated, intentional harm through messaging, social media, games or other online services where there is an imbalance of power. Online behaviour may also form part of harassment, stalking, coercive control, sexual violence, exploitation or abuse. The school records and responds to incidents consistently, supports those affected and considers risk beyond the immediate incident, including retaliation, wider sharing and impact on attendance or wellbeing.

Where a member of staff suspects that a device contains a nude, semi-nude or indecent image of a child, including an AI-generated or altered image, they must not deliberately view, copy, print, forward, store, save or delete it; ask a child to download or share it; investigate the details; or blame or shame anyone involved. The device should be secured in line with school procedures and the matter reported to the DSL immediately. If an image is seen accidentally, the member of staff records this and seeks DSL support.

The DSL follows current UKCIS guidance on sharing nudes and semi-nudes and DfE guidance on searching, screening and confiscation. Evidence is preserved where an offence may have occurred, and police or other agencies are contacted where required. Children are reassured that asking for help is the right action.

12. Searching and Confiscating Electronic Devices

Only the Headteacher or staff authorised by the Headteacher may search or examine an electronic device, and only in accordance with the school's behaviour arrangements and current statutory guidance. There must be a lawful and reasonable basis, such as a belief that the device has been or could be used to cause harm, disrupt the safe environment or commit an offence.

Before examining or erasing data, authorised staff consider safeguarding, privacy, proportionality and whether the material may be evidence. Material suspected to be evidence of an offence is not deleted and is passed to the police as soon as reasonably practicable. Any search involving a sexual image of a child follows the restrictions in section 11 and is led by the DSL.

13. Reporting and Responding to Concerns

Concerns must be reported promptly even when the person reporting is unsure how serious they are. Staff listen calmly, avoid leading or unnecessary questions, do not promise confidentiality, reassure the child and follow the school's safeguarding procedure. Immediate danger is reported to emergency services as well as the DSL.

Concern	Report to
Child safeguarding, grooming, exploitation, sexual content, harmful contact, radicalisation, online bullying or concern about an adult	DSL or deputy DSL immediately; record through CPOMS in line with safeguarding procedures.
Filtering or monitoring failure, harmful site accessible, wrongly blocked educational content, phishing, malware, compromised account or lost device	Designated IT support route; also the DSL and/or data-protection lead where safeguarding or personal data may be involved.
Personal-data loss, misdirected information or unauthorised disclosure	School data-breach route and data-protection lead without delay.
Staff conduct, professional-boundary or whistleblowing concern	Headteacher, Chair of Governors or the route set out in the relevant policy.

The response considers the child's safety and wishes, the nature and legality of the content or conduct, who may have received it, wider risks, evidence preservation, parental involvement and whether external agencies are required. Sanctions are proportionate and never replace safeguarding support. A genuine error reported promptly is considered differently from deliberate, concealed or reckless misuse.

14. Working with Parents and Carers

The school works in partnership with families because much online activity takes place beyond the school day and on privately owned devices. Parents and carers receive information about the school's curriculum, acceptable-use expectations, mobile-phone arrangements, filtering and monitoring, emerging risks and sources of support through the website, communications, meetings and events as appropriate.

Families are told what pupils are being asked to do online, including significant platforms or services and any school interaction through them. Concerns should normally be raised with the class teacher, Online Safety Lead, DSL or Headteacher according to their nature. Complaints are managed through the school's complaints procedure, but a safeguarding concern is acted upon immediately and is not delayed by that process.

15. Training and Professional Expectations

Online safety forms part of induction and safeguarding training for staff and relevant volunteers. All staff receive an update at least annually and additional information when risks, guidance or systems change. Training includes the four categories of risk, child-on-child abuse, sexual harassment, image-based abuse, radicalisation, AI and deepfakes, cyber security, filtering and monitoring responsibilities, professional boundaries, reporting routes and the additional vulnerability of some pupils.

The DSL and deputies maintain the online-safety knowledge required for their safeguarding role, including through formal safeguarding training at least every two years and updates at least annually. Governors receive appropriate safeguarding and online-safety training. The Online Safety Lead and IT support maintain role-specific knowledge and share relevant developments with staff.

16. Misuse and Breaches

Where a pupil misuses technology, the school follows the behaviour, acceptable-use and safeguarding procedures. The response depends on the circumstances, intent, impact and risk and may include education, restorative work, support, restricted access, confiscation or another proportionate consequence. Where a member of staff, governor, volunteer or contractor breaches this policy, the matter may be addressed through advice, training, restricted access, disciplinary, safeguarding or contractual procedures.

Illegal activity, serious harm, suspected abuse, significant data loss or a cyber-security incident may be referred to the police, local authority, regulator, insurer, service provider or another relevant agency. No one should investigate a serious incident beyond their authority or deliberately continue viewing illegal or harmful material.

17. Monitoring, Review and Assurance

The DSL and Online Safety Lead maintain and review records of online-safety concerns, actions and outcomes, using CPOMS and other approved systems as appropriate. Patterns are considered across safeguarding, behaviour, attendance, complaints, filtering alerts and technical incidents so that vulnerable pupils, repeated locations, devices, times or types of harm are identified.

Senior leaders complete an annual online-safety risk assessment and an annual review of filtering and monitoring. Findings inform curriculum planning, staff training, parent information, technical controls and the school improvement process. The Headteacher provides appropriate assurance to the Governing Body without disclosing unnecessary personal information.

This policy is reviewed annually and sooner following a serious incident, a change in statutory guidance or law, a significant technology or system change, or evidence that arrangements are not effective. Staff, pupils and parents or carers are consulted in proportionate ways, and material changes are communicated clearly.

18. Related Policies and Guidance

School policies and procedures: Child Protection and Safeguarding; Behaviour and Anti-Bullying; Staff Code of Conduct; Staff and Governor Acceptable Use of Technology; Pupil Acceptable Use Agreement; Data Protection and Privacy Notices; Records Management; Mobile Phones and Smart Technology; Social Media; Photography, Video and Image Use; Artificial Intelligence; RSHE; SEND; Equality; Complaints; Whistleblowing; Disciplinary; Cyber Security and Incident Response.

External guidance current at approval: Keeping Children Safe in Education 2026; DfE filtering and monitoring standards; DfE digital and technology standards; DfE guidance on teaching online safety, mobile phones, searching and confiscation, relationships and health education, bullying and preventing radicalisation; UKCIS guidance on sharing nudes and semi-nudes; ICO education and data-protection guidance; and National Cyber Security Centre guidance for schools.

19. Our Commitment

Holy Trinity and St John's Church of England Primary School is committed to a safe, respectful and purposeful digital culture. We will teach pupils the knowledge and confidence to make responsible choices, respond compassionately when someone needs help, and keep our systems and practice under review so that technology supports every child to flourish and become a light for others in the world.