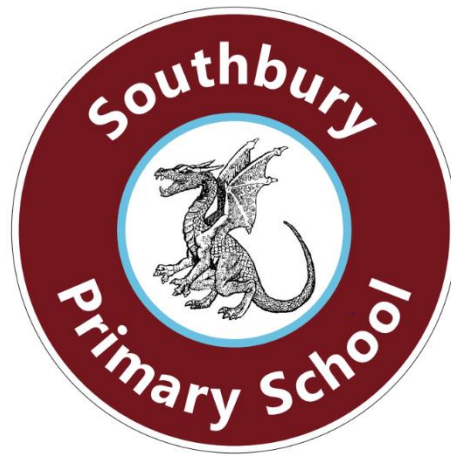


Southbury Primary School



Online Safety Policy September 2026

This policy should be read alongside the school's safeguarding, behaviour, anti-bullying, PSHE, data protection and Staff Code of Conduct arrangements.

Document Control

Policy	Online Safety Policy
Date	September 2026
Approved by	Governing Body
Review cycle	Annual, or sooner where significant changes occur
Next review	September 2027

Contents

1. Policy Statement and Overview
 2. What is Online Safety?
 3. Scope
 4. Aims
 5. Roles and Responsibilities
 6. Teaching and Learning
 7. Online Risks
 8. Safeguarding and Online Safety
 9. Cyberbullying, Online Abuse and Child-on-Child Abuse
 10. Artificial Intelligence and Emerging Technologies
 11. Managing Internet Access
 12. Filtering and Monitoring
 13. Information and Cyber Security
 14. Email and Online Communication
 15. Images, Video and Published Content
 16. Social Media
 17. Personal Data and Privacy
 18. Mobile Phones and Personal Devices
 19. Videoconferencing, Webcams and Online Platforms
 20. Acceptable Use
 21. Responding to Online Safety Incidents and Complaints
 22. Staff and Professional Use
 23. Parents and Carers
 24. Accessibility and Inclusion
 25. Training and Awareness
 26. Monitoring, Review and Annual Audit
 27. Links with Other Policies
 28. References and Guidance
- Appendix 1: Online Safety Annual Review Checklist

1. Policy Statement and Overview

Southbury Primary School recognises that digital technology and online services are an important part of children's education, communication and wider lives. Technology provides significant opportunities for learning, creativity and participation, but it can also expose children and adults to risks.

The school is committed to providing a safe digital environment in which pupils can use technology confidently, responsibly and respectfully. Online safety is an integral part of safeguarding and is taught, promoted and reinforced across school life.

This policy updates the school's previous Online Safety Policy and should be implemented alongside the school's wider safeguarding and pastoral arrangements.

2. What is Online Safety?

Online safety is the ability to use technology and online services safely, responsibly and respectfully. It includes understanding risks, making informed choices, protecting personal information, recognising harmful behaviour and knowing how and where to seek help.

Online risks can be considered under four broad areas:

- Content – being exposed to illegal, inappropriate or harmful material.
- Contact – harmful interaction with others online, including unwanted contact, grooming and exploitation.
- Conduct – behaviour online that causes or increases the risk of harm, including cyberbullying, harassment and the creation or sharing of inappropriate material.
- Commerce – risks such as scams, phishing, inappropriate advertising and other forms of financial exploitation.

Online risks change rapidly. The school will therefore review its arrangements regularly and consider emerging risks, including those associated with artificial intelligence and other developing technologies.

3. Scope

This policy applies to all pupils, staff, governors, volunteers, visitors, contractors and other adults using or accessing the school's digital systems or network.

It applies to technology and online activity undertaken on school premises, using school equipment or accounts, and to relevant online activity outside school where it affects the safety, wellbeing or education of pupils or the wider school community.

The policy applies to all school-managed devices, internet access, email, online platforms, applications, social media and other digital services approved for school use.

4. Aims

The aims of this policy are to:

- protect pupils and adults from inappropriate, harmful or illegal online content and activity;
- provide clear expectations for safe and responsible use of technology;
- teach pupils how to recognise online risks and seek help;
- promote respectful and responsible online behaviour;
- support pupils to develop critical thinking and evaluate information encountered online;
- ensure staff understand their safeguarding and professional responsibilities when using technology;

- maintain appropriate filtering, monitoring and cyber security arrangements;
- respond promptly and appropriately to online safety concerns;
- work with parents and carers to promote safe online experiences;
- ensure online safety arrangements are inclusive and accessible to pupils with additional needs.

5. Roles and Responsibilities

The Governing Body will provide appropriate oversight and assurance that effective online safety, filtering, monitoring and safeguarding arrangements are in place.

The Headteacher and senior leaders will ensure that online safety is embedded across school life, that appropriate procedures are implemented and that staff receive suitable information and training.

The Designated Safeguarding Lead and Deputy DSLs will oversee safeguarding concerns arising from online activity and ensure that staff follow the school's safeguarding procedures.

The member of staff responsible for online safety/digital technology will coordinate implementation of this policy, support staff and contribute to monitoring and review. The school will ensure that this responsibility is clearly allocated.

IT support and relevant technical staff will support the secure operation of systems, filtering, monitoring and access arrangements.

All staff are responsible for modelling safe and respectful online behaviour, supervising pupils appropriately, following acceptable use arrangements and reporting concerns promptly.

Pupils are expected to follow the school's online safety expectations, use technology respectfully and report anything that makes them feel uncomfortable, unsafe or concerned.

Parents and carers are encouraged to support the school's online safety expectations and to share relevant concerns with the school.

6. Teaching and Learning

Online safety education is embedded across the Computing curriculum and reinforced through PSHE, Relationships Education, Health Education, assemblies, safeguarding education and the wider curriculum.

Pupils will receive age-appropriate teaching about:

- respectful and responsible online behaviour;
- cyberbullying and online harassment;
- privacy and personal information;
- passwords and account security;
- online relationships and appropriate communication;
- recognising and reporting inappropriate contact;
- harmful and inappropriate online content;
- misinformation, disinformation and manipulated content;
- artificial intelligence and AI-generated content;
- sharing images and personal material;
- gaming, livestreaming and online communities;
- online scams and financial safety;
- digital footprints and online reputation;

- how and where to report concerns and seek help.

Teaching will be age-appropriate, inclusive and responsive to emerging risks affecting pupils. Staff will reinforce online safety expectations whenever pupils use technology.

7. Online Risks

The school recognises that pupils may encounter a wide range of online risks. These may include inappropriate or illegal content, pornography, harmful or distressing material, misinformation and disinformation, grooming, exploitation, cyberbullying, harassment, online hate or prejudice, harmful challenges, self-harm or suicide-related content, scams, phishing and financial exploitation.

Children may also experience pressure to communicate, share images, participate in online trends or use services that are not appropriate for their age.

The school will respond to concerns proportionately and in accordance with safeguarding, behaviour, anti-bullying and other relevant procedures.

8. Safeguarding and Online Safety

Online safety is an integral part of the school's safeguarding arrangements. Concerns arising from online activity will be considered alongside the school's wider safeguarding procedures.

Online safeguarding concerns may include, but are not limited to:

- grooming or exploitation;
- harmful or abusive content;
- sexual harassment or sexual abuse online;
- the sharing of nudes or semi-nudes, including manipulated or AI-generated images;
- cyberbullying or online harassment;
- online hate, prejudice or discriminatory behaviour;
- radicalisation or extremist content;
- harmful online challenges or hoaxes;
- self-harm or suicide-related content;
- scams, phishing or financial exploitation;
- inappropriate contact with adults or other children.

Any concern that may indicate that a child is at risk of harm must be reported to the Designated Safeguarding Lead or Deputy DSL without delay in accordance with the school's Safeguarding and Child Protection Policy.

Staff must not investigate safeguarding concerns themselves or promise confidentiality to a child.

9. Cyberbullying, Online Abuse and Child-on-Child Abuse

Cyberbullying is bullying carried out through digital technologies and may take place through messaging, social media, gaming platforms, group chats, websites or other online services.

Cyberbullying may include threats, harassment, exclusion, spreading rumours, sharing images or information without consent, impersonation, discriminatory abuse or repeated unwanted contact.

Reports of cyberbullying will be taken seriously and dealt with in accordance with the Anti-Bullying Policy and Behaviour Policy. Where a concern may constitute a safeguarding matter, it will also be referred to the DSL.

Online abuse between children may form part of wider child-on-child abuse. The school will respond in accordance with its safeguarding procedures and will consider the needs and safety of all children involved.

10. Artificial Intelligence and Emerging Technologies

The school recognises that artificial intelligence and other emerging technologies are developing rapidly and may present both educational opportunities and safeguarding risks.

Any use of generative artificial intelligence by pupils or staff must be appropriate, safe and consistent with the school's safeguarding, data protection and acceptable use arrangements.

Pupils will be taught, in an age-appropriate way, that information and images generated or altered using artificial intelligence may not be accurate or authentic. They will be supported to question, verify and critically evaluate information encountered online.

The school will consider safeguarding, data protection, copyright, intellectual property and educational implications before introducing new AI tools or services.

Pupils will be taught that AI can be used to create or manipulate images and other content and that this can cause harm. Concerns involving harmful or abusive AI-generated content will be treated as a safeguarding concern and reported in accordance with school procedures.

Staff must not enter confidential or personal information about pupils, families or staff into AI tools unless the tool has been approved for that purpose and its use is consistent with the school's data protection requirements.

11. Managing Internet Access

School internet access is provided to support teaching and learning and is subject to appropriate filtering, monitoring and supervision.

Pupils will be supervised when using the internet in accordance with their age, needs and the activity being undertaken.

Pupils will be taught what constitutes acceptable and unacceptable internet use and will be expected to follow the school's online safety and acceptable use expectations.

At Key Stage 1, internet access will be appropriately supervised and focused on approved materials. As pupils progress through the school, they will be taught how to search, evaluate and use online information responsibly.

Children will be encouraged to report anything online that makes them feel uncomfortable, worried or unsafe to a trusted adult.

12. Filtering and Monitoring

Southbury Primary School will maintain appropriate filtering and monitoring systems to help protect pupils and staff from illegal, inappropriate and potentially harmful online content.

Filtering is used to prevent access to inappropriate or harmful content. Monitoring is used to identify potentially concerning activity and support the school in responding to safeguarding concerns.

The school will ensure that:

- responsibility for filtering and monitoring is clearly allocated to appropriate school leaders, the DSL team and IT support;

- filtering and monitoring arrangements are reviewed at least annually and following significant changes to technology, systems or safeguarding risks;
- checks are carried out on relevant school-managed internet-connected devices and systems;
- records are kept of filtering and monitoring checks, concerns identified and actions taken;
- staff understand how to report concerns and how alerts are escalated;
- filtering is sufficiently effective to protect pupils without unreasonably restricting appropriate teaching and learning;
- safeguarding concerns identified through filtering or monitoring are referred to the DSL;
- governors receive appropriate assurance that filtering and monitoring arrangements are effective and regularly reviewed.

The school recognises that no filtering system can guarantee that inappropriate material will never be accessed. Staff remain responsible for supervising pupils and responding promptly to concerns.

13. Information and Cyber Security

School systems and devices will be protected through appropriate technical and organisational security measures.

Staff and pupils must keep passwords and account details secure and must not share passwords with others.

Accounts must only be used by the authorised user.

Suspicious emails, attachments, links, pop-ups or requests for personal information must be treated with caution and reported where appropriate.

School systems must be kept up to date with appropriate security updates and protection. Lost or stolen devices, suspected cyber incidents and data breaches must be reported promptly through the school's established procedures.

The school will undertake appropriate cyber security risk assessment and review arrangements regularly in line with current DfE digital and technology standards.

14. Email and Online Communication

Pupils may only use school-approved email accounts and online communication systems where authorised and supervised.

Pupils must communicate respectfully and must not send offensive, threatening or inappropriate messages or material.

Pupils should tell a member of staff if they receive an offensive, upsetting or inappropriate message.

Staff must use approved school accounts and systems when communicating on behalf of the school. Staff must maintain professional boundaries and must not use personal accounts to communicate privately with pupils.

Suspicious emails and attachments must not be opened unless it is safe and appropriate to do so.

15. Images, Video and Published Content

The school will follow its current consent and data protection arrangements when taking, storing or publishing photographs, videos or examples of pupils' work.

Images and videos will be selected and used appropriately, with consideration given to safeguarding, privacy, dignity and the context in which they are shared.

The school will not publish unnecessary personal information alongside images or work.

Staff will use school-approved devices and systems when taking photographs or videos of pupils and will follow the Staff Code of Conduct and data protection procedures.

Parents and carers will be informed about the school's arrangements for using images and work where appropriate.

16. Social Media

The school may use approved social media platforms and online communication channels to share information about school life and celebrate pupils' learning and achievements.

School social media accounts will be managed by authorised staff in accordance with safeguarding, data protection, image consent and professional conduct arrangements.

Personal social media accounts must not be used to communicate privately with pupils or to share confidential school information.

Staff should consider the potential impact of public online activity on their professional role and must follow the Staff Code of Conduct.

Pupils will be taught age-appropriate guidance about social media, including privacy, respectful communication, reporting concerns and the risks associated with sharing personal information.

17. Personal Data and Privacy

Personal data will be collected, recorded, processed, stored and shared in accordance with applicable data protection legislation, including the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025.

Staff and pupils must not publish or share personal information about themselves or others through school systems unless authorised and appropriate.

The school will minimise the amount of personal information shared online and will use approved systems for storing and transferring school information.

Staff must follow the school's data protection procedures and seek advice where they are unsure whether information can be shared.

18. Mobile Phones and Personal Devices

Pupils' use of mobile phones and other personal devices will be managed in accordance with the school's current mobile phone arrangements.

Personal devices must not be used in school to photograph, record or communicate with pupils unless specifically authorised as part of an approved school activity.

Staff will use school-approved devices for photographing or recording pupils and will follow the Staff Code of Conduct.

Personal devices must not be connected to or used to bypass school filtering or security arrangements.

19. Videoconferencing, Webcams and Online Platforms

Videoconferencing and webcam use will only take place for approved educational or organisational purposes and will be appropriately supervised.

Only school-approved platforms should be used for online meetings or learning.

Staff should consider privacy, participant access, recording arrangements, chat functions and safeguarding before using an online meeting platform with pupils.

Recordings must only be made where there is a clear educational or organisational purpose, appropriate authorisation and suitable arrangements for storage and deletion.

20. Acceptable Use

Pupils, staff and other authorised users are expected to use school technology safely, responsibly and respectfully.

Users must not attempt to access inappropriate, illegal or unauthorised material; bypass security or filtering; misuse another person's account; deliberately damage systems; or use technology to bully, harass, threaten or discriminate against others.

Users must report concerns, inappropriate content, security issues or accidental access to unsuitable material to a member of staff or through the school's established reporting arrangements.

Acceptable use expectations will be explained to pupils and staff and reinforced regularly. Where the school uses separate acceptable use agreements, these will be reviewed alongside this policy.

21. Responding to Online Safety Incidents and Complaints

Online safety incidents will be dealt with promptly, proportionately and in accordance with the nature of the concern.

Concerns may be managed through the Behaviour Policy, Anti-Bullying Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct, Data Protection procedures or other relevant school procedures.

Where a concern involves a child protection or safeguarding issue, it must be referred to the DSL without delay.

Concerns about staff misuse must be reported in accordance with the Staff Code of Conduct and safeguarding procedures.

Technical incidents, including suspected cyber attacks, data breaches or compromised accounts, must be reported promptly to the appropriate school leader and IT support.

Records of significant incidents will be maintained and used to identify patterns, emerging risks and areas for further action.

22. Staff and Professional Use

All staff must comply with the school's Staff Code of Conduct when using school technology, digital systems, email, social media and online services.

Staff must maintain professional boundaries when communicating electronically and must not use personal accounts to communicate privately with pupils.

Staff must not share confidential school information through personal accounts or unapproved platforms.

Staff must report safeguarding concerns, inappropriate online behaviour, data breaches and misuse of school systems through the appropriate school procedures.

Staff should model respectful, critical and responsible online behaviour and reinforce online safety expectations when pupils use technology.

23. Parents and Carers

Parents and carers play an important role in supporting children to use technology safely. The school will provide information and signposting to support families where appropriate.

Parents and carers will be made aware of the school's online safety expectations and relevant reporting arrangements.

The school will work with parents/carers when online activity outside school has a significant impact on a pupil's safety, wellbeing or education.

The school will maintain current online safety resources for parents/carers and will update signposting as services and platforms change.

24. Accessibility and Inclusion

The school will seek to ensure that online safety education, reporting routes and digital resources are accessible to all pupils, including pupils with SEND, communication needs or other barriers to access.

Staff will consider reasonable adjustments and individual needs when teaching online safety and responding to concerns.

Accessibility features should not be unnecessarily blocked by generic filtering or security arrangements where they are required to support pupils' access to learning.

25. Training and Awareness

Staff will receive appropriate online safety and safeguarding information and training. Training will reflect current and emerging risks and the responsibilities of different staff members.

Staff who have responsibility for filtering, monitoring, digital technology or safeguarding will receive appropriate role-specific information and support.

Pupils will receive regular online safety education through the curriculum and wider school life.

Parents and carers will be offered appropriate information and signposting to support safe use of technology at home.

26. Monitoring, Review and Annual Audit

The effectiveness of this policy will be monitored through filtering and monitoring reviews, safeguarding records, online safety incidents, pupil voice, staff feedback, parent/carers feedback, curriculum review and relevant technical assurance.

The policy will be reviewed annually or sooner where significant changes occur in legislation, statutory guidance, technology, online risks or school arrangements.

The school will maintain an annual online safety review checklist to support governance and identify actions for improvement.

27. Links with Other Policies

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Mental Health and Wellbeing Policy
- PSHE Policy and curriculum
- Staff Code of Conduct
- Data Protection / Privacy arrangements
- Mobile Phone Policy, where applicable
- Attendance Policy, where relevant
- Equality and Inclusion arrangements
- Acceptable Use Agreements, where applicable.

28. References and Guidance

This policy has been informed by current Department for Education guidance and standards, including:

- Keeping Children Safe in Education 2026.
- Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance, in force from 1 September 2026.
- DfE Meeting digital and technology standards in schools and colleges – Filtering and monitoring: core standard.
- DfE Meeting digital and technology standards in schools and colleges – Cyber security: core standard.
- DfE Meeting digital and technology standards in schools and colleges – Digital accessibility.
- Relevant UK Council for Internet Safety guidance and age-appropriate online safety resources.

The school will take account of updates to statutory guidance, DfE standards and emerging online safety risks when reviewing this policy.

Appendix 1: Online Safety Annual Review Checklist

Governance and policy

Check	Yes / No	Action / Evidence
Responsibility for online safety is clearly allocated.		
Policy has been reviewed and updated where necessary.		
Governors have received appropriate assurance about online safety arrangements.		
Online safety risks are considered within the school's safeguarding arrangements.		

Filtering and monitoring

Check	Yes / No	Action / Evidence
Annual filtering and monitoring review completed.		
Relevant school-managed devices and systems included in checks.		
Checks and actions are recorded.		
Filtering blocks harmful and inappropriate content without unreasonably restricting teaching and learning.		
Monitoring arrangements meet the safeguarding needs of the school.		
Alerts and concerns are appropriately escalated to the DSL or relevant staff.		

Curriculum

Check	Yes / No	Action / Evidence
Online safety is taught through Computing and reinforced through PSHE, Relationships Education and Health Education.		
Teaching reflects current and emerging online risks.		
Teaching is age-appropriate and accessible.		
Pupils know how to report concerns and seek help.		

Safeguarding

Check	Yes / No	Action / Evidence
Online safeguarding concerns are recorded and managed through safeguarding procedures.		
Staff understand how to report online safeguarding concerns.		
Cyberbullying, online exploitation, harmful content and child-on-child online abuse are appropriately addressed.		
Staff know what to do if a child reports an online concern.		

Technology and AI

Check	Yes / No	Action / Evidence
New technologies and online platforms are risk assessed before use where appropriate.		
Generative AI risks and opportunities are considered.		
Staff understand expectations for safe use of AI and confidential information.		
Cyber security arrangements are reviewed appropriately.		

Staff

Check	Yes / No	Action / Evidence
Staff have received appropriate online safety training.		
Staff understand professional online boundaries.		
Staff know how to report safeguarding, technical and data protection concerns.		
Staff use approved devices and systems appropriately.		

Parents and carers

Check	Yes / No	Action / Evidence
Parents/carers receive appropriate online safety information.		
Current signposting is available.		

Families know how to raise online safety concerns with the school.		
--	--	--

Pupil voice and inclusion

Check	Yes / No	Action / Evidence
Pupil voice has been considered.		
Online safety reporting routes are accessible to pupils.		
Provision considers SEND and other individual needs.		
Emerging concerns identified by pupils are considered in school planning.		