Sancton Wood School

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

Online Safety Policy (September 2025)

This policy is for the whole school inc EYFS

Written by: RS/ HS/ GU/ HOS	September 2025
Current version no:	
Reviewed:	September 2025
Approved by the Governing Body:	September 2025
Next review:	September 2026

1. Introduction

It is the duty of Sancton Wood School to ensure that every pupil in its care is safe; the same principles apply to the digital world as they do to the real world. Information technology and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse, radicalisation, and exposure to harmful content including misinformation and disinformation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites and search engines
- Email and instant messaging
- Blogs and social networking sites
- Chat rooms and online forums
- Music and video downloads
- Gaming sites and platforms
- Text messaging and picture messaging
- Video calls and conferencing
- Podcasting and streaming services
- Online communities via games consoles
- Mobile internet devices such as smartphones and tablets
- Artificial Intelligence (AI) and generative AI tools
- Virtual and augmented reality platforms

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

This policy, supported by the Acceptable Use Policy for all staff, visitors and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. This policy is compliant with the Online Safety Act 2023, DfE Filtering and Monitoring Standards for Schools and Colleges (2024), and Keeping Children Safe in Education (2024).

1.1 Related School Policies

This policy is linked to the following school policies:

- Safeguarding and Child Protection
- Staff Behaviour and Code of Conduct
- Health and Safety
- Behaviour Management
- Anti-Bullying
- Acceptable Use Policy
- Social Media Policy
- Data Protection and Privacy
- PSHE (Personal, Social, Health and Economic Education)
- Teaching Online Safety Policy

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and emerging threats including those posed by artificial intelligence tools.

At Sancton Wood School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, interactive whiteboards, digital video equipment, etc.) as well as all devices owned by

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smartphones, etc.) under our Bring Your Own Device (BYOD) provisions.

All devices accessing the school network, whether school-owned or personal, must meet the same safety standards and filtering requirements as outlined in this policy.

3. Legal Framework and Compliance

This policy is designed to ensure compliance with:

- Online Safety Act 2023 - addressing illegal content, harmful content, and platform responsibilities
- Keeping Children Safe in Education (2024) - statutory safeguarding guidance
- DfE Filtering and Monitoring Standards for Schools and Colleges (2024) - technical requirements for educational settings
- Data Protection Act 2018 and UK GDPR - privacy and data handling requirements
- Children Act 1989 - child welfare obligations
- Education Act 2002 - safeguarding duties
- Prevent Duty Guidance (2023) - counter-terrorism obligations
- UK Safer Internet Centre Guidelines (2025) - appropriate filtering and monitoring definitions

4. Roles and Responsibilities

4.1 The Governing Body

The governing body has **strategic responsibility** for ensuring that:

- Appropriate and effective filtering and monitoring systems are in place
- This policy is reviewed annually and updated as required
- Staff receive adequate training about e-safety and filtering/monitoring responsibilities
- The school meets its statutory obligations under relevant legislation
- Annual reviews of filtering and monitoring provision are conducted
- Data Protection Impact Assessments (DPIAs) are completed for monitoring systems
- Resources are allocated for effective online safety measures

The governing body will review this policy at least annually, taking into account the annual filtering and monitoring review, emerging threats, and changes in technology or legislation.

4.2 Principal and Senior Leadership Team

The Principal has overall responsibility for the safety of members of the school community, including e-safety. The Senior Leadership Team has **operational responsibility** for:

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

- Day-to-day management of filtering and monitoring systems
- Ensuring staff understand procedures and policies for e-safety breaches
- Making decisions about content blocking and system configurations
- Training staff on their filtering and monitoring responsibilities
- Coordinating with the Designated Safeguarding Lead on online safety matters
- Documenting decisions and maintaining records of system effectiveness
- Ensuring business continuity plans include online safety considerations

4.3 Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for:

- Understanding the school's filtering and monitoring systems and processes
- Taking lead responsibility for online safety within the broader safeguarding framework
- Providing governors with assurance that filtering and monitoring systems are working effectively
- Liaising with senior leadership on online safety strategy and incidents
- Coordinating responses to online safety incidents in line with safeguarding procedures
- Working with IT staff to ensure technical and safeguarding concerns are addressed
- Reporting patterns of concern to relevant authorities

4.4 IT Staff and Technical Support

The school's technical staff (including our third-party provider Smoothwall) have responsibility for:

- Maintaining a safe technical infrastructure
- Implementing and managing filtering and monitoring systems
- Keeping abreast with rapid technological developments and emerging threats
- Ensuring system security, data protection, and effective operation
- Training teaching and administrative staff in IT use
- Monitoring internet and email usage according to approved protocols
- Reporting inappropriate usage to the Director of Operations and DSL
- Conducting regular system updates and security patches
- Maintaining illegal URL filter lists that cannot be disabled or modified
- Blocking VPNs, proxy services, and other bypass methods
- Ensuring safe search is enabled and locked across all systems

4.5 Teaching and Support Staff

All staff are required to sign the Acceptable Use Policy before accessing the school's systems. Staff responsibilities include:

- Creating a talking and listening culture to address e-safety issues daily
- Understanding their role in the filtering and monitoring framework
- Reporting safeguarding and technical concerns through appropriate channels
- Incorporating e-safety education across the curriculum
- Being alert to signs of online abuse, radicalisation, or harmful behaviour
- Following escalation procedures for online safety incidents
- Understanding the acceptable use of AI and generative AI tools in educational settings

4.6 Pupils

Pupils are responsible for:

- Using school IT systems in accordance with the Acceptable Use Policy
- Reporting misuse of IT systems to staff immediately
- Understanding and following online safety guidance
- Not attempting to bypass filtering or monitoring systems
- Treating online interactions with the same respect as face-to-face interactions
- Seeking help from trusted adults when they encounter concerning content or behaviour online

4.7 Parents and Carers

Sancton Wood School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. Parents and carers are responsible for:

- Endorsing the school's Acceptable Use Policy
- Supporting online safety education at home
- Understanding that our filtering extends to home use through Smoothwall's provision
- Communicating any concerns about their child's online experiences
- Engaging with school-provided resources and training opportunities
- Monitoring and guiding their child's internet use outside of school hours

We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise hopes that parents will feel able to share any concerns with the school.

5. Technical Infrastructure and Systems

5.1 Filtering Systems

The school operates comprehensive filtering systems provided by Smoothwall, which:

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

- Block illegal content: Including child sexual abuse material, terrorism-related content, and other illegal material as defined by the Online Safety Act 2023
- Filter harmful and inappropriate content: Including but not limited to:
    - Content that is bullying, abusive, or hateful
    - Content depicting or encouraging serious violence or injury
    - Dangerous stunts and challenges
    - Exposure to harmful substances
    - Age-inappropriate sexual content
    - Misinformation and disinformation
    - Extremist and radicalisation content
    - Self-harm and suicide-related content
- Maintain illegal URL filter lists that cannot be disabled or modified by any user, including system administrators
- Block VPNs, proxy services, and other circumvention tools to prevent filter bypass
- Enable safe search by default across all search engines, locked and unchangeable by users
- Cover all devices including school-owned equipment and personal devices (BYOD) to the same safety standards
- Provide real-time content scanning for emerging threats and new harmful content
- Allow appropriate educational content without unreasonably impacting teaching and learning

5.2 Monitoring Systems

The school implements monitoring systems that:

- Track user activity on school devices and networks in real-time
- Generate alerts for suspicious or inappropriate behaviour
- Provide detailed reports that can track incidents to specific devices or users
- Enable prompt response to flagged incidents through defined escalation procedures
- Support both automated and manual monitoring including staff observation of screens
- Comply with data protection requirements through completed DPIAs
- Maintain audit trails for investigation and safeguarding purposes

5.3 Home Filtering Provision

Through our partnership with Smoothwall, filtering protection extends to **school-owned devices that are taken home by pupils**, ensuring:

- Consistent protection on school devices across both school and home environments

- Continued filtering during remote learning periods when using school-issued equipment
- Support for parents in maintaining online safety when pupils use school devices at home

Please note: This filtering does **not** apply to personal home devices or home networks. Parents are encouraged to implement their own parental controls and safety measures on personal devices used at home.

5.4 Artificial Intelligence and Generative AI

Before approving the use of any AI tools or generative AI platforms, the school will assess:

- The level to which our filtering systems can block AI content in real time
- Built-in safety features of AI tools and data protection implications
- The need for specific policies around the use of generative AI systems
- Our ability to generate reports of AI tool usage within the school
- Educational benefits versus potential risks
- Age-appropriateness and curriculum alignment

All AI tools used in school must comply with our filtering and monitoring standards and data protection requirements.

6. Education and Training

6.1 Staff Training and Awareness

New Staff Induction: All new staff receive information on Sancton Wood School's e-safety and Acceptable Use policies as part of their induction, including:

- Understanding of filtering and monitoring systems and their responsibilities
- Recognition of online safety risks and indicators of concern
- Procedures for reporting and escalating online safety incidents
- Use of AI tools and generative AI platforms in educational settings

Ongoing Training: All staff receive regular information and training on e-safety issues through INSET training and internal meetings. This includes:

- Annual updates on emerging threats and technologies
- Changes to legislation and guidance
- Updates to filtering and monitoring procedures
- Recognition of signs of online abuse, radicalisation, and harmful behaviour

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

- Training on the educational use of new technologies including AI tools

All supply staff receive information about e-safety as part of their safeguarding briefing on arrival at school.

6.2 Pupil Education

Curriculum Integration: IT and online resources are used increasingly across the curriculum. E-safety guidance is provided to pupils on a regular and meaningful basis through:

- Computing lessons: Technical understanding of online safety, digital citizenship, and responsible use
- PSHE education: Emotional and social aspects of online interactions, relationship building, and personal safety
- Cross-curricular opportunities: Subject-specific online safety considerations
- Assembly presentations: Whole-school awareness of current issues and themes
- Peer education programmes: Older pupils supporting younger ones

Age-Appropriate Content: From Year 1 onwards, pupils receive age-appropriate education covering:

- Understanding of appropriate and inappropriate online behaviour
- Recognition of online risks and how to respond
- How and when to seek support
- Digital citizenship and respect for others online
- Understanding of the law as it applies to online behaviour
- Critical evaluation of online information and media literacy
- Awareness of artificial intelligence and how to use AI tools safely and responsibly

From Year 7 onwards, additional content includes:

- Recognition of online sexual exploitation, stalking, and grooming
- Understanding of relevant laws including data protection and intellectual property
- Respect for other people's information and images
- Understanding the risks and implications of sharing personal information and images
- Advanced critical thinking skills for evaluating online content
- Understanding of digital footprints and online reputation management

Reporting and Support: Pupils understand that they can report concerns to:

- The Designated Safeguarding Lead
- Any member of staff at the school
- Parents, carers, and trusted adults outside school
- External agencies such as CEOP and Childline

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

6.3 Parent and Community Education

The school recognises that not all parents and guardians may feel equipped to protect their children when they use electronic equipment at home. We therefore provide:

- Regular information sessions for parents about online safety and current digital trends
- External specialist presentations advising about e-safety and practical protective steps
- Written guidance and resources sent home and available on the school website
- Individual support for families experiencing online safety challenges
- Information about home filtering provided through our Smoothwall partnership
- Guidance on AI tools and generative AI that children may encounter or use

7. Use of Internet and Email

7.1 Staff Guidelines

Acceptable Use: Staff must not access social networking sites, personal email, or any website unconnected with school work or business from school devices or whilst teaching/in front of pupils. Personal access may only be made from staff members' own devices whilst off premises.

Professional Standards: When accessing social media from off-school premises, staff must use extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

Communication Monitoring: Staff should be aware that email communications through the school network and staff email addresses are monitored in accordance with our monitoring policy and DPIA.

Incident Reporting: Staff must immediately report to IT support the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, or bullying in nature. Staff must not respond to any such communication and must remain alert to fraudulent emails.

Professional Communication: Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent/carer using any personal email address or social media platform.

Prohibited Activities: Any online communications must not knowingly or recklessly:

- Place a child or young person at risk of harm, or cause actual harm
- Bring Sancton Wood School into disrepute
- Breach confidentiality or copyright
- Breach data protection legislation

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

- Constitute discrimination, bullying, or harassment
- Include offensive or derogatory content based on protected characteristics
- Involve adding school pupils or parents as social network 'friends'

7.2 Pupil Guidelines

System Protection: There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments are blocked automatically. If this causes problems for school work/research purposes, pupils should contact their class/form teacher for assistance.

Reporting Procedures: Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, or bullying in nature. Such communications should be immediately reported to a member of staff.

Responsible Posting: Pupils are expected to think carefully before posting any information online, or reposting or endorsing content created by others. Content posted should not be inappropriate, offensive, or likely to cause embarrassment to the individual or others.

Incident Response: Pupils must report any accidental access to materials of a violent or sexual nature directly to a member of staff. Deliberate access to inappropriate materials will be recorded and dealt with under the school's Behaviour Policy.

Monitoring Awareness: Pupils should be aware that all internet usage via the school's systems and WiFi network is monitored in accordance with our monitoring policy.

AI Tool Usage: Use of artificial intelligence and generative AI tools must be approved by staff and conducted in accordance with school guidelines for educational purposes only.

8. Data Storage, Processing, and Protection

8.1 GDPR and Data Protection Compliance

The school takes compliance with the Data Protection Act 2018 and UK GDPR seriously. All online safety measures are implemented with due regard to data protection principles and individual privacy rights.

Data Protection Impact Assessments (DPIAs): The school has completed DPIAs for all monitoring systems to ensure that:

- Processing is lawful, fair, and transparent
- Data is collected for specified, explicit, and legitimate purposes
- Personal data is adequate, relevant, and limited to what is necessary
- Information is accurate and kept up to date
- Data is kept no longer than necessary

- Appropriate security measures are in place

Lawful Basis for Processing: The school's lawful basis for monitoring and filtering activities is:

- Public task: Performance of a task carried out in the public interest (education and safeguarding)
- Vital interests: Protection of life and safety of pupils and staff
- Legal obligation: Compliance with safeguarding and educational legislation

8.2 Password Security

Individual Accounts: Pupils and staff have individual school network logins, email addresses, and cloud storage folders. All users are regularly reminded of the need for password security.

Password Requirements: All pupils and staff must:

- Use strong passwords (minimum eight characters containing upper- and lower-case letters and numbers)
- Change passwords annually or when prompted by security protocols
- Not write passwords down or share them with others
- Report suspected password compromise immediately

Multi-Factor Authentication: Where available and appropriate, multi-factor authentication is enabled to provide additional security layers.

9. Device Management and Security

9.1 Examining Electronic Devices

Authority to Search: The Principal, and any member of staff authorised by the Principal (as set out in the behaviour policy), can carry out a search and confiscate any electronic device where they have reasonable grounds for suspecting it:

- Poses a risk to staff or pupils
- Is identified in school rules as a banned item for which a search can be carried out
- Contains evidence relating to an offence

Search Procedures: Before conducting a search, the authorised staff member will:

- Assess the urgency of the search and consider risks to other pupils and staff
- Explain to the pupil why they are being searched and how the search will be conducted
- Give the pupil opportunity to ask questions about the process
- Seek the pupil's cooperation where possible

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

Examination of Content: Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device where they believe there is a 'good reason' to do so, specifically where they reasonably suspect the device has been or could be used to:

- Cause harm to individuals
- Undermine the safe environment of the school or disrupt teaching
- Commit an offence

Safeguarding Considerations: If inappropriate material is found, the Head of School, in conjunction with the DSL, will decide on appropriate responses. If there are images, data, or files that staff reasonably suspect are likely to put a person at risk, safeguarding responses will be prioritised.

Indecent Images Protocol: If a staff member suspects a device may contain indecent images of children, they will:

- Not view the image
- Confiscate the device immediately
- Report the incident to the DSL immediately
- Follow guidance from UKCIS on sharing nudes and semi-nudes

Legal Compliance: Any searching will be carried out in line with:

- DfE guidance on searching, screening, and confiscation
- UKCIS guidance on sharing nudes and semi-nudes
- The school's behaviour and safeguarding policies

10. Annual Review and System Assessment

10.1 Mandatory Annual Review

Governing Body Responsibility: The governing body ensures that filtering and monitoring provision is reviewed at least once every academic year as part of a wider online safety review.

Review Participants: The annual review is conducted by:

- Members of the senior leadership team
- The Designated Safeguarding Lead
- IT support staff (including Smoothwall representatives where appropriate)
- The responsible governor

Review Components: The annual review assesses:

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

- Current provision analysis: Identifying what filtering and monitoring systems are in place
- Gap analysis: Determining areas for improvement or upgrade
- Risk assessment: Evaluating students' and staff's specific needs and risk profiles
- System effectiveness: Testing and validating filtering and monitoring performance
- Emerging threats: Considering new technologies, platforms, and risks
- Compliance check: Ensuring adherence to current legislation and guidance
- Cost-benefit analysis: Reviewing system costs against safeguarding benefits
- User feedback: Gathering input from staff, pupils, and parents
- Incident analysis: Reviewing patterns of online safety incidents and system responses

Risk Profile Considerations: The review specifically considers how students' risk profiles inform filtering and monitoring approaches, including:

- Age and developmental stage of pupils
- Presence of special educational needs and disabilities (SEND)
- English as an additional language (EAL) considerations
- Looked-after children and previously looked-after children
- Pupils with social workers or child protection plans
- Specific vulnerabilities or safeguarding concerns

Documentation and Reporting: Results of the annual review are:

- Recorded in writing with clear recommendations
- Made available to those entitled to inspect the information
- Reported to the governing body with action plans for improvements
- Used to update policies, procedures, and technical configurations
- Shared with relevant staff and stakeholders as appropriate

10.2 Continuous Monitoring and Improvement

Ongoing Assessment: Beyond the annual review, the school continuously monitors:

- System performance and effectiveness
- Emerging technologies and threats
- Changes in legislation and guidance
- Feedback from users and stakeholders
- Incident patterns and trends

Technology Updates: The school stays current with technological developments through:

- Regular communication with Smoothwall and other providers
- Participation in professional networks and training opportunities
- Monitoring of government guidance and industry best practice

- Testing of new tools and platforms before implementation

11. Incident Response and Misuse

11.1 Incident Classification

Immediate Response Required:

- Discovery of illegal content (child sexual abuse material, terrorism content)
- Evidence of grooming, sexual exploitation, or radicalisation
- Serious threats to individuals or school community
- Significant safeguarding concerns

Standard Response:

- Inappropriate content access (accidental or deliberate)
- Cyberbullying or online harassment
- Breach of acceptable use policies
- Technical security incidents

Minor Incidents:

- Educational guidance opportunities
- First-time policy breaches with no harm caused
- Technical support needs

11.2 Response Procedures

Immediate Safety: The school will not tolerate illegal activities or activities that are inappropriate in a school context. Illegal activity will be reported to the police and/or Local Safeguarding Children Board (LSCB). Where a child or young person is at risk as a consequence of online activity, assistance may be sought from the Child Exploitation and Online Protection Centre (CEOP).

Incident Management: All incidents of misuse or suspected misuse must be dealt with by staff in accordance with:

- The school's safeguarding policy and procedures
- This online safety policy
- The behaviour management policy
- The anti-bullying policy where appropriate

Recording and Reporting:

- All incidents are recorded using the school's incident reporting system
- Serious incidents are reported to the DSL immediately
- Patterns of behaviour are monitored and analysed
- Parents are informed of incidents involving their children
- External agencies are contacted when required by legislation or safeguarding needs

Sanctions and Support: The school will impose appropriate sanctions on pupils who misuse technology to bully, harass, or abuse others, in line with our behaviour and anti-bullying policies. This may include:

- Temporary or permanent removal of internet access
- Temporary or permanent removal of specific devices or software
- Withdrawal of privileges
- Referral to external agencies for support
- In serious cases, involvement of police or social services

Restorative Approaches: Where appropriate, the school employs restorative approaches to help pupils:

- Understand the impact of their actions
- Develop empathy for those affected
- Learn strategies to prevent future incidents
- Rebuild relationships and trust

12. Supporting Pupils and Families

12.1 Victim Support

Immediate Support: Pupils who experience online abuse, harassment, or exposure to harmful content receive:

- Immediate safety measures and risk assessment
- Emotional support from trained staff
- Access to counselling services where appropriate
- Ongoing monitoring and protection measures
- Clear information about next steps and support available

Specialist Referrals: The school works with external agencies to provide specialist support, including:

- Child and Adolescent Mental Health Services (CAMHS)
- Local authority children's services
- Police specialist units
- Voluntary sector organisations (e.g., NSPCC, Childline)

- Online safety specialist organisations

12.2 Family Support

Parental Involvement: Parents are involved in online safety incidents through:

- Immediate notification of serious incidents
- Discussion of support needs and strategies
- Provision of resources and guidance for home safety
- Referral to specialist support services where needed
- Ongoing communication about progress and concerns

Home-School Partnership: The school works with families to:

- Align online safety approaches between home and school
- Provide consistent messages and expectations
- Share resources and training opportunities
- Support parents in managing technology at home
- Address specific family needs and circumstances

13. Special Considerations

13.1 Vulnerable Groups

Pupils with SEND: Additional considerations for pupils with special educational needs and disabilities include:

- Adapted online safety education materials
- Increased supervision and monitoring where appropriate
- Recognition of additional vulnerabilities online
- Coordination with SENCo and specialist staff
- Individual risk assessments and support plans

Looked-After Children: Specific support for looked-after children includes:

- Coordination with virtual school head and social workers
- Recognition of additional vulnerabilities and trauma history
- Careful consideration of information sharing and confidentiality
- Prioritised access to support services
- Stability and consistency in online safety approaches

Children with Social Workers: For children with allocated social workers:

- Information sharing with relevant professionals

- Coordinated safeguarding approaches
- Recognition of existing vulnerabilities and risks
- Prioritised response to online safety concerns
- Regular review of support and protection measures

13.2 Remote Learning Considerations

Home Learning Environment: During periods of remote learning:

- Filtering and monitoring extend to home devices through Smoothwall provision
- Video conferencing and online platform safety measures are enforced
- Staff training covers remote teaching safety considerations
- Pupils receive specific guidance on home learning safety
- Parents are provided with additional support and resources

Platform Security: All remote learning platforms and tools:

- Meet the school's security and safety standards
- Include appropriate privacy and data protection measures
- Are regularly reviewed for safety and effectiveness
- Include clear reporting mechanisms for concerns
- Provide appropriate supervision and monitoring capabilities

14. Complaints and Concerns

14.1 Complaint Procedures

As with all issues of safety at Sancton Wood School, if a member of staff, pupil, or parent/carer has a complaint or concern relating to e-safety, prompt action will be taken to address it.

Initial Response:

- Complaints should be addressed to the Head in the first instance
- Urgent safeguarding concerns should be reported to the DSL immediately
- Technical issues should be reported to IT support
- All complaints will be acknowledged within 24 hours

Investigation Process:

- Appropriate investigation will be undertaken based on the nature of the complaint
- External agencies will be involved where required
- All parties will be kept informed of progress
- Outcomes and actions will be clearly communicated

Appeals Process: If complainants are not satisfied with the initial response:

- They may appeal to the governing body
- External mediation services may be accessed
- Regulatory bodies may be contacted where appropriate
- All appeals will be handled fairly and transparently

14.2 Continuous Improvement

Learning from Incidents: The school uses complaints and incidents to:

- Identify areas for policy and procedure improvement
- Update training and education programmes
- Enhance technical systems and controls
- Strengthen partnerships with families and external agencies
- Share learning with other schools and professionals

15. Implementation and Communication

15.1 Policy Dissemination

Staff: All staff members:

- Receive a copy of this policy during induction
- Are trained on policy requirements and procedures
- Sign acknowledgement of understanding and compliance
- Receive updates when the policy is revised
- Have access to support and guidance for implementation

Pupils: Pupils are made aware of online safety expectations through:

- Age-appropriate presentations and discussions
- Integration into curriculum and PSHE programmes
- Regular reminders and updates
- Clear reporting mechanisms and support pathways
- Opportunities to contribute to policy development

Parents and Community: The school ensures parents and the wider community are informed through:

- Publication on the school website
- Information sessions and presentations
- Written communications and newsletters
- Individual discussions when relevant

- Opportunities for feedback and input

15.2 Monitoring and Evaluation

Policy Effectiveness: The effectiveness of this policy is monitored through:

- Regular incident analysis and pattern identification
- Feedback from staff, pupils, and parents
- Annual review outcomes and recommendations
- Compliance audits and assessments
- Comparison with sector best practice and guidance

Continuous Development: The school commits to:

- Regular policy updates in response to emerging threats and guidance
- Ongoing professional development for staff
- Investment in appropriate technology and systems
- Collaboration with other schools and professional networks
- Engagement with research and best practice development

Appendices

Appendix A: Key Contacts

Internal Contacts:

- Principal: [Contact details]
- Designated Safeguarding Lead: [Contact details]
- IT Support: [Contact details]
- Chair of Governors: [Contact details]

External Emergency Contacts:

- Police: 999 (emergency) / 101 (non-emergency)
- Local Authority Designated Officer (LADO): [Contact details]
- Local Authority Children's Services: [Contact details]
- CEOP: www.ceop.police.uk/safety-centre

Support Services:

- Childline: 0800 1111
- NSPCC Helpline: 0808 800 5000
- UK Safer Internet Centre: www.saferinternet.org.uk

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

- Internet Watch Foundation: www.iwf.org.uk

Appendix B: Technical Specifications

Smoothwall Filtering System:

- Content categories blocked and allowed
- Update frequency and management
- Home filtering provision details
- Reporting and monitoring capabilities
- VPN and proxy blocking specifications

Monitoring System Requirements:

- Real-time alerts and thresholds
- Reporting capabilities and retention periods
- Privacy protection measures
- Staff access levels and permissions
- Integration with safeguarding procedures

Appendix C: Educational Resources

Age-Appropriate Online Safety Curricula:

- EYFS and Key Stage 1 resources
- Key Stage 2 progression and topics
- Key Stage 3 and 4 comprehensive programmes
- Sixth form and young adult considerations
- Cross-curricular integration opportunities

Staff Training Materials:

- Induction training modules
- Annual update presentations
- Incident response procedures
- Technical system training
- Legal and policy update briefings

Parent and Community Resources:

- Home safety guidance documents
- Technology setup and monitoring advice
- Age-appropriate conversation starters
- External support and advice sources

2 St. Paul's Rd, Cambridge CB1 2EZ
01223 471703
office.prep@sanctonwood.co.uk
www.sanctonwood.co.uk

- Current trend and threat awareness materials