



SPARKEN HILL
ACADEMY

Online Safety Policy

Revision Record				
Rev	Date Issued	Prepared By	Approved	Comments
1.2	Feb 2021	RTL		
1.3	February 2026	RTL	26.02.26	Significantly updated with latest guidance and KCSiE & RSHE guidance

1. POLICY STATEMENT

1.1 Our Commitment

At Sparken Hill Academy, we are committed to ensuring that all pupils, staff, and members of our school community can use technology safely and responsibly. We recognise that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of abuse and other risks online, as well as face to face

We maintain an attitude of "**it could happen here**" and adopt a **zero-tolerance approach** to online abuse and harmful behaviour.

1.2 Legal Framework

This policy fulfils our statutory duties under:

- Keeping Children Safe in Education (KCSIE) 2025
- The Education Act 2011
- The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- The Equality Act 2010
- Relationships, Sex and Health Education (RSHE) statutory guidance (September 2025) Relationships and Sex Education Statutory Guidance

1.3 Scope

This policy applies to all members of Sparken Hill Academy community (including staff, pupils, volunteers, parents/carers, visitors, and governors) who have access to our digital technology on or off site.

2. ROLES AND RESPONSIBILITIES

2.1 The Governing Board

The governing board has strategic leadership responsibility for the school's safeguarding arrangements and must make sure the school's policies, procedures and training are effective and comply with legislation

The governing board will:

- Ensure online safety is a running and interrelated theme throughout the school's safeguarding policies and procedures
- Appoint a board member responsible for the school's safeguarding arrangements

- Ensure appropriate filtering and monitoring systems are in place and regularly review their effectiveness
- Review the DfE's filtering and monitoring standards and discuss with IT staff and service providers what more needs to be done to support the school to meet the standards
- Ensure this policy is reviewed annually

2.2 The Headteacher

The Headteacher will:

- Ensure all staff understand this policy and their responsibilities
- Ensure appropriate training and support is provided
- Take overall responsibility for online safety provision
- Ensure this policy is implemented effectively

2.3 The Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Acting as the named point of contact on all online safeguarding issues
- Liaising with relevant agencies regarding online safety concerns
- Ensuring all staff understand how to recognise and respond to online safety concerns
- Maintaining records of online safety incidents
- Monitoring online safety incident logs
- Coordinating the school's response to online safety incidents

2.4 All Staff

All staff should provide a safe environment in which children can learn and know about (and feel confident to use) school safeguarding systems

All staff must:

- Read and adhere to this policy and the acceptable use agreements
- Report any online safety concerns immediately to the DSL
- Model safe and responsible online behaviour
- Maintain an attitude of 'it could happen here' regarding online risks
- Embed online safety messages in their teaching where appropriate
- Be aware that technology is a significant component in many safeguarding and wellbeing issues

2.5 Pupils

Pupils are responsible for:

- Reading, understanding, and adhering to the acceptable use agreement
- Respecting others online and reporting concerns
- Understanding that online behaviour should reflect our school values
- Seeking help from a trusted adult if they encounter concerning content or behaviour online

2.6 Parents and Carers

Parents and carers are expected to:

- Support the school's online safety approaches
- Discuss online safety at home and set appropriate boundaries
- Report concerns to the school
- Reinforce positive online behaviours

3. ONLINE SAFETY EDUCATION

3.1 Curriculum Provision

Online safety is embedded throughout our curriculum, particularly through:

Computing Curriculum: Progressive online safety teaching across all year groups covering:

- The Education for a Connected World framework of digital knowledge and skills for different ages and stages Relationships Education, Relationships and Sex Education and Health Education
- Safe searching and evaluating online content
- Understanding digital footprints
- Recognising fake websites and checking URLs
- Password security and personal information protection

RSHE Programme: From September 2026, our RSHE curriculum will include age-appropriate teaching on:

- Online relationships, including the risks of communicating online with people they don't know
- How to critically evaluate online information and recognise risks such as misinformation, disinformation and conspiracy theories
- The impact of viewing harmful content online
- Respectful online behaviour
- Sexting and sharing of images Relationships Education, Relationships and Sex Education and Health Education

Assemblies and PSHE: Regular age-appropriate sessions covering current online safety issues.

3.2 Teaching Approach

We will:

- Use **Thinkuknow** resources from the National Crime Agency (NCA) and Child Exploitation Online Programme (CEOP) Relationships Education, Relationships and Sex Education and Health Education
- Ensure teaching is age-appropriate and considers pupils' developmental stages
- Adapt teaching for pupils with SEND to ensure accessibility
- Regularly update content to reflect emerging risks
- Encourage open discussion and critical thinking

3.3 Staff Training

All staff will receive:

- Online safety training at induction, which is regularly updated
- An understanding of the expectations, applicable roles and responsibilities around filtering and monitoring
- Annual safeguarding updates including online safety developments
- Information about emerging risks and trends

The DSL will:

- Undertake training on their role and update this at least every 2 years
- Refresh their knowledge and skills at least once a year through e-bulletins, meeting other DSLs, and reading about safeguarding developments

4. ONLINE SAFETY RISKS

4.1 The Four Categories of Risk

We consider the 4 areas of online safety risk – content, contact, conduct and commerce:

Content: Exposure to illegal, inappropriate or harmful material, including:

- Misinformation, disinformation (including fake news), and conspiracy theories
- Pornography and sexual content
- Violence and gore
- Hate speech and discriminatory content
- Self-harm and suicide content
- Extremist materials

Contact: Being subjected to harmful online interaction with others, including:

- Grooming and sexual exploitation
- Online bullying and harassment
- Radicalisation
- Contact from strangers
- Inappropriate adult contact

Conduct: Personal online behaviour that increases the likelihood of harm, including:

- Sharing personal information
- Cyberbullying others
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos
- Sexting
- Online reputation damage
- Copyright infringement

Commerce: Risks related to online commercial activities, including:

- Exposure to inappropriate advertising
- Online gambling
- In-app purchases
- Financial scams
- Identity theft

4.2 Specific Safeguarding Concerns

Staff should be aware that children can abuse other children online, including through:

- Cyber-bullying, prejudice-based and discriminatory bullying
- Sexual harassment, including online sexual harassment
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos
- Upskirting

Staff must also be alert to:

- Child sexual exploitation (CSE) and child criminal exploitation (CCE)
- Radicalisation and extremism
- Domestic abuse (which children may witness or experience online)

5. MANAGING ONLINE SAFETY

5.1 Filtering and Monitoring Systems

The governing board must make sure appropriate filtering and monitoring systems are in place and regularly review their effectiveness

Our Approach:

- We use **Smoothwall** to filter inappropriate content
- We use **Smoothwall Monitor** to monitor online activity
- We use the DfE's 'plan technology for your school' service to self-assess our school against the DfE's standards and receive personalised recommendations
- Our filtering and monitoring requirements apply to the use of generative AI in education
- Systems are reviewed annually and adjusted based on identified risks
- We balance protection with avoiding 'over-blocking' that restricts legitimate educational content

Monitoring Process:

- Designated staff review monitoring alerts daily
- Concerns are escalated to the DSL immediately
- Serious concerns trigger our safeguarding procedures
- Pupils and parents are made aware that school devices and networks are monitored

5.2 Use of Personal Devices and Mobile Phones

Staff:

- Personal mobile phones must not be used in teaching areas during lesson time
- Staff should use school devices for all work-related communication
- Personal devices must not be used to take photographs or videos of pupils
- Staff must follow our Staff Code of Conduct regarding social media

Pupils:

- Mobile phones are not permitted in school for pupils in Years R-6
- If pupils bring devices to school (e.g., for after-school clubs), they must be handed to the office on arrival
- Smart watches must be in 'school mode' with communication features disabled
- Any breach will result in confiscation and parent contact

Visitors:

- Visitors must not use mobile phones in areas where pupils are present
- Photography is only permitted with prior permission from the Headteacher

5.3 Use of School Devices and Networks

- All school devices have filtering and monitoring software installed
- Pupils may only access approved websites and applications
- Personal email accounts and social media should not be accessed on school devices
- Any attempt to bypass security measures will be treated as a serious breach
- All users must log off when finished and report any security concerns

5.4 Social Media

School Accounts:

- Official school social media accounts are managed by designated staff
- All posts are approved by the Headteacher or senior leader
- Comments are moderated and inappropriate content removed immediately
- We do not accept friend/follow requests from current pupils

Staff Personal Accounts:

- Staff should maintain professional boundaries online
- Staff must not accept current pupils or their parents as 'friends' on personal accounts
- Staff should review privacy settings regularly
- Staff must not post anything that could bring the school into disrepute
- Any safeguarding concerns identified through social media must be reported to the DSL

Pupils:

- Pupils under 13 should not have social media accounts (in line with most platforms' terms of service)
- We educate pupils about safe and responsible social media use
- We encourage parents to monitor their children's online activity

5.5 Online Communication with Pupils and Parents

- All communication must be professional and transparent
- Staff must use school email addresses and approved platforms only
- Communication should take place during school hours where possible
- One-to-one online communication should be avoided; copy in another staff member where necessary

- Video calls should be conducted through approved school platforms with appropriate safeguards
- Staff must not share personal contact details with pupils or parents

5.6 Remote Learning

When remote learning is necessary:

- We use Google Classroom / Google Drive as our approved platform
- Staff and pupils must follow acceptable use agreements
- Video lessons should be recorded where possible
- Pupils should ensure appropriate backgrounds and dress
- Parents/carers should supervise younger pupils during video sessions
- Any concerns must be reported immediately to the DSL

6. RESPONDING TO ONLINE SAFETY INCIDENTS

6.1 Reporting Procedures

If staff have concerns about a child, they should act immediately, follow the child protection policy, and speak to the DSL (or deputy) as soon as they can

All incidents must be reported to the DSL, including:

- Accessing or sharing inappropriate content
- Online bullying or harassment
- Sharing of nude or semi-nude images
- Contact from unknown adults
- Radicalisation concerns
- Data breaches
- Any safeguarding concern with an online element

Recording:

- All incidents must be logged on CPOMS
- Include: date, time, individuals involved, nature of incident, action taken
- Keep a log of all concerns, discussions and decisions made, and the reasons for those decisions

6.2 Responding to Specific Incidents

Sharing of Nude or Semi-Nude Images:

- Follow UKCCIS sexting advice for schools on preventative education and managing reports of sexting Relationships Education, Relationships and Sex Education and Health Education
- Never view, copy, print, or share the images

- Report immediately to the DSL
- Consider whether police involvement is necessary
- Support all pupils involved (both those who shared and received images)

Cyberbullying:

- Take all reports seriously
- Investigate promptly and thoroughly
- Apply sanctions in line with behaviour policy
- Support victim and address perpetrator behaviour
- Involve parents of all pupils involved
- Consider whether the incident meets the threshold for police involvement

Inappropriate Content:

- Ensure the pupil is safe and supported
- Report to DSL immediately
- Consider whether content needs reporting to authorities (e.g., IWF, CEOP)
- Review filtering systems to prevent future access
- Provide appropriate support and education

Online Radicalisation:

- Report immediately to DSL
- Follow Prevent procedures
- Contact local Prevent coordinator
- Do not investigate independently

6.3 Working with Parents and Carers

We use regular contact with parents and carers to reinforce the importance of online safety, including making parents and carers aware of what we ask children to do online

We will:

- Inform parents promptly of any incidents involving their child
- Provide clear information about actions taken
- Offer guidance and support for managing online safety at home
- Run parent workshops on online safety topics
- Share resources and information through newsletters and our website

7. DATA PROTECTION AND SECURITY

7.1 Data Protection Principles

Staff are aware of their obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018, and that data protection regulations do not prevent information sharing for the purpose of keeping children safe

We will:

- Process personal data lawfully, fairly, and transparently
- Collect data only for specified, explicit purposes
- Ensure data is adequate, relevant, and limited to what is necessary
- Keep data accurate and up to date
- Retain data only as long as necessary
- Ensure appropriate security measures are in place

7.2 Information Security

- All devices are password protected
- Passwords must be strong and changed regularly
- Sensitive data is encrypted
- USB drives and portable devices are encrypted and password protected
- Staff must not remove or copy personal data without authorisation

This policy will be reviewed annually.