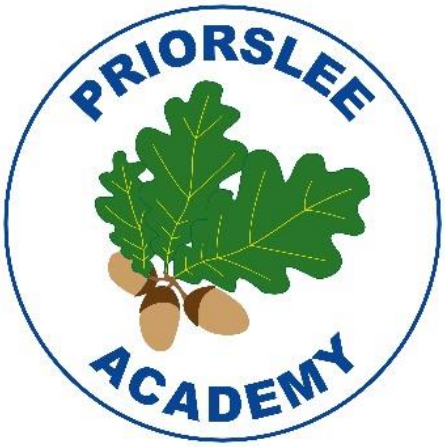
# Policy for Online Safety

*Reviewed by Jodie Cooper*

*September 2025*




# Online Safety Policy

## Aims

Mighty Oaks Academy Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective, whole-school approach to online safety that both protects and educates the school community in its use of technology, including mobile and smart devices
- Establish clear procedures to identify, intervene and escalate online safety concerns where appropriate

## The Four Key Categories of Risk

Our approach to online safety addresses the following categories of risk:

Content

Exposure to illegal, inappropriate or harmful content, including:

- Pornography
- Fake news and misinformation
- Racism, misogyny and hate content
- Self-harm and suicide related material
- Antisemitism
- Radicalisation and extremism

Contact

Harmful online interaction, including:

- Peer-to-peer pressure
- Commercial exploitation
- Adults posing as children to groom or exploit

Conduct

Personal online behaviour that may cause harm, including:

- Online bullying
- Sharing explicit images or content
- Non-consensual sharing of images
- Inappropriate communication

Commerce

Risks such as:

- Online gambling
- Inappropriate advertising
- Phishing and financial scams

In line with KCSIE, the school also recognises:

- The growing risk of misinformation and disinformation, including conspiracy theories

- Emerging risks linked to artificial intelligence (AI) such as deepfakes, AI-generated misinformation and algorithmic manipulation

Teaching will support pupils to:

- Critically evaluate online information
- Understand how AI systems work at an age-appropriate level
- Recognise and respond safely to online risks

## Legislation and Guidance

This policy is based on:

- Keeping Children Safe in Education
- DfE guidance on:
  - Teaching online safety in schools
  - Preventing and tackling bullying and cyber-bullying
  - Relationships and Health Education
  - Searching, screening and confiscation
- DfE guidance on preventing radicalisation
- Education Acts 1996, 2006 and 2011
- Equality Act 2010

The policy also reflects:

- National Curriculum Computing Programmes of Study
- RSHE statutory guidance, updated to include digital safety, misogyny awareness and mental health
- Equality and Human Rights Commission guidance where supporting gender-questioning pupils

## Roles and Responsibilities

### Governing Board

The Governing Board:

- Holds the Head of School to account for implementation
- Receives reports and monitors online safety practice
- Ensures safeguarding and online safety are embedded across school policies

Online Safety Link Governor: **Katie Handy**

All governors will:

- Read and understand this policy
- Comply with acceptable use agreements

- Ensure safeguarding education is adapted for vulnerable pupils and those with SEND

Head of School

The Head of School is responsible for:

- Day-to-day implementation of this policy
- Ensuring staff understand and follow online safety procedures
- Liaising with the DSL and governors
- Taking appropriate action following incidents

Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety, including:

- Managing and responding to online safety concerns
- Logging incidents appropriately
- Monitoring staff use of systems
- Overseeing cyber-bullying responses
- Delivering staff training and updates
- Liaising with external agencies
- Reporting termly to leadership and governors

All Staff and Volunteers

All staff and volunteers are responsible for:

- Understanding and following this policy
- Enforcing acceptable use agreements
- Reporting online safety concerns promptly
- Responding to reports of online abuse or harassment
- Maintaining an attitude of *"it could happen here"*

Parents and Carers

Parents are expected to:

- Raise concerns with the Head of School or DSL
- Support and reinforce acceptable use expectations
- Engage with school guidance on online safety

The school will share resources and guidance through:

- School communications
- The school website

Visitors and Community Members
Visitors using school ICT systems must comply with this policy and acceptable use requirements.

## Educating Pupils About Online Safety

Online safety education is embedded across the curriculum.
Key Stage 1 pupils will learn to:

- Use technology safely and respectfully
- Keep personal information private
- Ask for help when concerned

Key Stage 2 pupils will learn to:

- Use technology responsibly and respectfully
- Recognise acceptable and unacceptable behaviour
- Understand how to report concerns

By the end of Key Stage 2, pupils will understand:

- Online and offline behaviour expectations
- Risks of online relationships
- Safe boundaries and reporting routes
- Use and sharing of data and information

Teaching will be adapted for pupils with SEND or additional vulnerability.

## Educating Parents About Online Safety

The school will:

- Share information on filtering and monitoring systems
- Inform parents about online platforms used in school
- Encourage dialogue about online safety at home

Concerns should initially be raised with the Head of School or DSL.

## Cyber-Bullying

Definition
Cyber-bullying is repeated, intentional harm using online platforms where there is a power imbalance.
Preventing and Responding

- Pupils are taught how to recognise and report cyber-bullying
- Incidents are handled in line with the Behaviour Policy
- Evidence is preserved and investigated

- Police referrals are made where illegal material is involved

Acceptable Use of the Internet

All users must follow acceptable use agreements.

Use of the internet must be:

- Educational or professional only
- Safe, appropriate and monitored

Pupils Using Mobile Devices

- Pupils may bring devices to school but must not use them during:
  - Lessons
  - Clubs or school activities
- Breaches may result in confiscation and sanctions

Staff Using Work Devices Off-Site

Staff must:

- Keep devices secure and password-protected
- Ensure encryption and software updates
- Use devices for work purposes only

Security concerns should be reported immediately.

Responding to Misuse

- Pupil misuse is managed under the Behaviour Policy
- Staff misuse is addressed through disciplinary procedures
- Serious incidents may be reported to the police

The school uses the DfE Filtering and Monitoring Self-Assessment Tool.

Training

- All new staff receive online safety training
- All staff receive annual refresher training
- DSLs update knowledge regularly
- Governors receive safeguarding training
- Volunteers receive appropriate induction

## Review

This policy will be reviewed annually or sooner if required by legislative change or school need.