

Upper Wharfedale Primary Federation

Online Safety Policy



Date approved: September 2026

Review cycle: Annual

Next review: September 2027

1. Statement of Intent

Upper Wharfedale Primary Federation is committed to safeguarding and promoting the welfare of all children. We recognise that digital technologies are an integral part of children's lives and provide significant opportunities for learning, communication and creativity. However, we also recognise that technology can expose children and adults to risks.

Online safety is a safeguarding issue and is embedded within the Federation's wider safeguarding culture. We aim to create an environment where pupils, staff and families can use technology safely, responsibly and confidently.

The Federation is committed to:

- Protecting children from online harm.
- Promoting safe and responsible use of technology.
- Developing pupils' digital literacy and resilience.
- Supporting staff and parents to understand current online risks.
- Maintaining effective filtering, monitoring and cyber-security arrangements.
- Responding effectively to online safety concerns and incidents.
- Preparing pupils for an increasingly digital world.

Our approach reflects the four areas of online risk:

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

- Pornography
- Racism

- Misogyny
- Extremist content
- Self-harm and suicide content
- Misinformation and disinformation
- Deepfakes and manipulated media

Commented [KM1]: do we need to include misandry?

Contact: Harmful interactions online, including:

- Grooming
- Exploitation
- Bullying
- Coercion
- Harmful contact from adults or peers
- Unsafe interactions with AI systems and chatbots

Conduct: Behaviour that causes harm online, including:

- Bullying
- Harassment
- Sharing inappropriate content
- Image-based abuse
- Online discrimination
- Misuse of artificial intelligence

Commerce: Risks involving money, scams or commercial exploitation, including:

- Fraud
- Gambling
- Phishing
- Financial scams
- Inappropriate advertising

2. Legal Framework

This policy has due regard to:

Keeping Children Safe in Education (KCSIE 2026)

Working Together to Safeguard Children

Online Safety Act 2023

UK GDPR

Data Protection Act 2018

DfE Filtering and Monitoring Standards

DfE Teaching Online Safety in Schools Guidance

This policy should be read alongside

- Child Protection and Safeguarding Policy
- Child-on-Child Abuse Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Social Media Policy
- Cyber Security Policy
- Data Protection Policy
- Remote Education Policy
- Safe Use of AI Policy
- Acceptable Use Agreements

3. Roles and Responsibilities

An appointed Senior Leadership Team member holds strategic responsibility for overseeing filtering and monitoring systems, working in close collaboration with the DSL and IT technical support to conduct and log regular reviews.

Commented [KM2]: do we need to say what a DSL is?

Governing Board

The Governing Board is responsible for:

- Ensuring online safety arrangements are effective.
- Ensuring appropriate safeguarding and online safety policies are in place.
- Reviewing this policy annually.
- Receiving assurance regarding filtering and monitoring arrangements.
- Safeguarding Governor to be updated regularly by DSLs on Filtering and monitoring
- Ensuring staff receive appropriate safeguarding and online safety training.
- Maintaining awareness of emerging online risks.

Headteacher

The Headteacher will:

- Promote a whole-school approach to online safety.
- Ensure the policy is implemented consistently.
- Support the DSL in delivering effective digital safeguarding.
- Ensure staff training is provided and updated.
- Oversees the technical day-to-day operation of filtering and monitoring.
- Ensure appropriate resources are available to manage online safety effectively.
- Designated Safeguarding Lead (DSL)

The DSL will:

- Lead on online safety matters.
- Coordinate responses to online safety concerns.
- Maintain records of incidents and actions taken.
- Monitor trends and emerging risks.
- Liaise with external agencies where necessary.
- Ensure online safety is embedded within safeguarding practice.
- Support staff, pupils and families where concerns arise.

Staff

Staff will:

- Act as positive role models.
- Follow all relevant policies and procedures.
- Understand their safeguarding responsibilities.
- Report concerns immediately.
- Promote safe and responsible use of technology.

Pupils

Pupils are expected to:

- Use technology safely and responsibly.
- Follow acceptable use expectations.
- Treat others respectfully online.
- Report concerns to a trusted adult.

4. Managing Online Safety

The Federation adopts a whole-school approach to online safety.

We recognise that technology can be used to facilitate:

- Bullying
- Child-on-child abuse
- Sexual harassment
- Grooming
- Criminal exploitation
- Radicalisation
- Image-based abuse
- Fraud
- Harmful online behaviour

Online safety is embedded within:

- Safeguarding procedures
- Curriculum planning
- Staff training
- Behaviour expectations
- Parent engagement

Any online safety concern will be treated as a safeguarding concern where appropriate and managed in accordance with safeguarding procedures.

5. Online Harm, Exploitation and Abuse

The Federation recognises that the internet may be used to facilitate abuse and exploitation.

Grooming

Staff will remain alert to signs that a child may be experiencing grooming through online platforms, gaming services, social media or messaging applications.

Child Sexual Exploitation (CSE)

Online technologies may be used to exploit children through coercion, manipulation or abuse.

Child Criminal Exploitation (CCE)

Children may be targeted online by individuals seeking to exploit them for criminal purposes.

Radicalisation

Children may encounter extremist material online or become vulnerable to radicalisation through digital platforms.

Staff concerns regarding any form of exploitation or abuse must be reported immediately to the DSL.

6. Child-on-Child Abuse and Online Bullying

The Federation maintains a zero-tolerance approach to child-on-child abuse, harmful sexual behaviour and online bullying.

Online behaviours may include:

- Bullying
- Harassment
- Sexual harassment
- Hate incidents
- Sharing of inappropriate images
- Image-based abuse including the sharing nudes and semi-nudes (including self-generated, AI-generated or manipulated deepfake content)
- Pressuring others to share content

The Federation recognises that image-based abuse may involve:

- Edited images
- Manipulated photographs
- Deepfakes
- AI-generated imagery

Creating, sharing or threatening to share intimate images may constitute a safeguarding concern and will be managed in accordance with safeguarding procedures.

All incidents will be investigated appropriately and support provided to those affected.

7. Emerging Technology and Artificial Intelligence

The Federation recognises the rapidly evolving nature of digital technology and the opportunities and risks associated with artificial intelligence (AI).

Emerging technologies may include:

- Generative AI tools
- Deepfake technologies
- AI chatbots
- Image-generation software

- Virtual assistants
- Anonymous communication platforms

The Federation will:

- Assess risks before introducing new technologies.
- Ensure staff understand emerging online risks.
- Provide education about AI and digital literacy.
- Maintain appropriate safeguards.
- Review new technologies regularly.

Pupils will be taught that AI-generated content may be inaccurate, misleading or manipulated.

The misuse of AI, including creating or sharing harmful, misleading or manipulated content, may be treated as a safeguarding concern.

8. Online Safety Education

Curriculum

Online safety is embedded throughout the curriculum and delivered through:

- Computing
- Relationships Education
- PSHE
- Assemblies
- Safeguarding activities

Pupils will learn:

- How to stay safe online.
- How to seek help.
- How to behave respectfully.
- How to identify online risks.
- How to evaluate information critically.
- How to recognise misinformation and manipulated content.
- How to use emerging technologies responsibly.

The curriculum will address:

- Cyberbullying
- Consent
- Respectful relationships

- Online scams
- Artificial intelligence
- Digital citizenship
- Misogyny and harmful stereotypes

Staff Training

All staff will receive regular safeguarding and online safety training.

Training may include:

- Emerging online risks
- Child-on-child abuse
- Image-based abuse
- Filtering and monitoring
- Artificial intelligence
- Reporting procedures

Parent Engagement

The Federation values partnership with parents and carers.

- Support may be provided through:
- Newsletters
- Information evenings
- Online resources
- Updates regarding emerging online risks

Parents are encouraged to discuss online safety regularly with their children and seek support where required.

9. Use of Technology

All users are expected to use technology safely, legally and responsibly.

The Federation may provide access to:

- Laptops
- Tablets
- Internet services
- Educational platforms
- Email systems

All use of school technology must comply with relevant acceptable use agreements.

Mobile Phones and Smart Technology

Pupils are not permitted to use personal mobile phones during the school day.

Where a pupil requires a mobile phone for travel arrangements:

The phone must be handed into the school office at the start of the day, where they will be kept in a locked drawer.

The phone will be returned at the end of the school day.

Smart watches are not permitted. The ban on smart technology and smartwatches includes fitness trackers and wearables (such as Fitbits) if they are capable of receiving notifications, text messages, calls, or connecting to the internet. Basic fitness trackers that only count steps or monitor health data without communication capabilities may be permitted, at the discretion of the Headteacher.

Any unauthorised devices brought onto site may be confiscated in line with the Federation's Behaviour Policy and retained securely until an appropriate adult can collect them.

The Federation will review arrangements annually in response to emerging safeguarding risks.

10. Acceptable Use Agreements

The Federation will maintain Acceptable Use Agreements (AUAs) for:

- Pupils
- Staff
- Governors
- Volunteers, where appropriate

All users must read, understand and agree to the relevant Acceptable Use Agreement before accessing Federation systems and devices.

The Acceptable Use Agreements set out expectations regarding:

- Safe use of technology
- Online behaviour
- Social media use
- Use of artificial intelligence
- Data protection
- Cyber security
- Reporting concerns

Failure to comply with the relevant agreement may result in disciplinary action and, where appropriate, safeguarding action.

11. Filtering, Monitoring and Cyber Security

The Federation maintains appropriate filtering and monitoring arrangements to support safeguarding and protect users from harmful content.

The Federation recognises that robust cyber security is an essential element of safeguarding, protecting sensitive pupil data, school systems, and users from digital threats and malicious breaches."

Commented [KM3]: delete?

The Federation has a lead DSL (working alongside the DSL and Headteacher) to oversee the day-to-end management, testing, and logging of filtering and monitoring system.

The Federation will maintain a formal, written log of all filtering and monitoring checks, evidencing that systems are tested and functioning effectively across all internet-connected devices and federation sites."

Commented [KM4]: delete?

Filtering and monitoring systems will:

- Meet statutory requirements.
- Support safeguarding practice.
- Be proportionate to risk.
- Be reviewed regularly.
- Be reviewed formally at least annually.
- Findings from annual reviews will be reported to governors.

The Federation also maintains cyber-security arrangements to protect systems, data and users.

Staff and pupils are expected to:

- Protect passwords.
- Report suspicious activity.
- Follow cyber-security procedures.
- Use school systems appropriately.

12. Reporting Concerns

Any online safety concern involving a pupil must be reported immediately to the DSL.

Concerns may include:

- Bullying
- Grooming
- Exploitation
- Harassment
- Radicalisation
- Harmful content
- Sharing of images
- Deepfakes
- AI-generated abuse
- Self-harm concerns

All incidents will be recorded and managed in line with the Child Protection and Safeguarding Policy.

Where necessary, concerns may be referred to external agencies including Children's Social Care, the Police, CEOP or other relevant services.

13. Monitoring and Review

The Federation recognises that technology and online risks continue to evolve.

This policy will be reviewed

- Annually.
- Following significant safeguarding incidents.
- Following major legislative or guidance changes.

Reviews will consider:

- Emerging technologies.
- Artificial intelligence.
- Deepfake technologies.
- Online **misogyny**.
- National safeguarding guidance.
- Filtering and monitoring effectiveness.
- Feedback from staff, pupils and governors.

The Federation remains committed to maintaining a proactive and responsive approach to online safety to ensure that all members of the school community are protected and supported in the digital world.

Approved by Governing Board: _____

Commented [KM5]: misogyny?

Chair of Governors: _____

Date: _____

Appendix One Acceptable User Agreements

Pupil Acceptable Use Agreement

My Online Safety Promise I want to be a safe and responsible digital citizen at the Upper Wharfedale Primary Federation. I agree to:

- **Be Kind:** I will never use technology to bully, hurt, or embarrass others. I will treat everyone with respect.
- **Protect My Privacy:** I will not share my personal details (like my address or phone number) or my passwords with anyone.
- **Stay Safe:** I will only visit websites I know are safe and meant for learning. If I see something that makes me feel worried, uncomfortable, or sad, I will close the screen and tell a trusted adult immediately.
- **Be Honest:** I will not try to bypass school security or use AI to copy someone else's work. I know that if I use AI, I must be honest about it.

- **Ask Permission:** I will only use devices (laptops/tablets) when my teacher tells me to. I will not bring personal mobile phones or smartwatches to school unless the Headteacher has given special permission.
- **Report Concerns:** If I am worried about something I see online, or if someone is being unkind to me or someone else, I will tell a teacher, my parent, or a trusted adult straight away.

I understand that if I do not follow these rules, I may lose my right to use school technology.

Signed _____

Professional Online Safety and ICT Agreement

As a member of staff at Upper Wharfedale Primary Federation, I understand that my use of technology must always support the safety, welfare, and best interests of children. I agree to comply with all aspects of this agreement:

1. Safeguarding and Online Safety

- I will immediately report any online safety concerns, including child-on-child abuse, incidents involving the making or sharing of nudes and semi-nudes, extremist content, or grooming indicators, to the DSL/Headteacher.
- I will maintain professional boundaries in all digital communication. I will not 'friend', follow, or communicate with pupils on personal social media accounts or via personal messaging apps.

2. System Security and Passwords

- I will never share my system passwords or account credentials with anyone.
- I will ensure all workstations and devices are locked or logged out when left unattended.

- I will not attempt to install unauthorised software, games, or applications on school hardware.

3. Filtering and Monitoring

- I will not attempt to bypass, disable, or circumvent the school's filtering and monitoring systems. I understand these are critical statutory safeguarding tools.
- I will remain vigilant and report any unusual technical behaviour or content gaps observed on school networks.

4. Data Protection (UK GDPR)

- I will handle all sensitive pupil and staff data in strict accordance with UK GDPR and the Federation's Data Protection Policy.
- I will ensure personal data is stored securely and never left exposed on desks, unencrypted drives, or accessible public spaces.

5. Use of Artificial Intelligence (AI)

- I will use AI tools (such as Microsoft Copilot) in compliance with the Federation's *Safe Use of AI Policy*.
- I will **never** input identifiable pupil data, personal information, or confidential safeguarding logs into public or unapproved AI models.
- I will maintain human oversight, rigorously checking any AI-generated resources or communications for accuracy, bias, and appropriateness before use.

6. Use of Personal Devices

- I understand that personal devices (such as smartphones, tablets, or smartwatches) must **never** be used to photograph, video, or record pupils or school activities. All media must be captured using school-owned equipment.
- I will not store pupil data, personal identifiable information, or confidential school documents on personal devices.
- If personal devices are brought onto site, I will keep them out of sight and silenced during teaching and learning time to ensure full focus on pupil supervision.
- I will not use personal devices or personal phone numbers to communicate directly with pupils or parents; all professional communication must go through official federation channels.

7. Professional Role Modelling

- I will model responsible digital citizenship, ensuring that my own online conduct, language, and use of technology set a positive example for pupils at all times.

Agreement Acknowledgment

Name of Staff Member: _____

Signature: _____

Date: _____

Governor Digital and Data Agreement

As a Governor of Upper Wharfedale Primary Federation, I recognise that I have access to sensitive information and a responsibility to model good practice. I agree to:

- **Secure Communication:** I will use official school-provided email addresses (where available) for all school business. I will not use personal email for sensitive or confidential pupil/staff information.
- **Data Protection:** I will ensure all hard-copy and digital documents containing personal data are stored securely and destroyed/deleted when no longer required, in line with UK GDPR.

- **Safeguarding Oversight:** I will maintain my understanding of current online safety risks (including AI and image-based abuse) to ensure the Governing Board can hold the school to account effectively.
- **Confidentiality:** I will keep all board discussions and confidential school documents private, both offline and in digital spaces (including social media).
- **System Integrity:** I will not attempt to access systems or data that fall outside the scope of my governor responsibilities.
- **Reporting:** I will immediately report any loss of a device or suspected data breach to the Headteacher or the Data Protection Officer.

I understand that my access to school systems is granted based on my commitment to these responsibilities and the protection of our school community.

Signed _____