FOREST OF DEAN COMMUNITY SCHOOLS FEDERATION

PARKEND PRIMARY & YORKLEY PRIMARY

Online Safety and Acceptable Users Policy

2026 - 2028

Ratified: March 2026

Contents:

Statement of intent

The Forest of Dean Community Schools Federation understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The purpose of the Federation's online safety policy is to:

- Have robust processes in place to safeguard and protect all members of the federation's community online.
- Deliver an effective approach to online safety of pupils, staff, volunteers and governors.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards practice when using technology.
- Identify clear procedures to identify, intervene and escalate an incident, where appropriate.

The implementation of this policy is the responsibility of all teaching staff and should be overseen and monitored by the Executive Headteacher, DSL, and the governors.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Additional risks include AI-generated content such as deepfakes, fake or manipulated imagery, and exposure to misinformation, disinformation and conspiracy theories, as identified in KCSIE 2025.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. **Legal framework**

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- UK GDPR & Data Protection Act 2018
- DfE (2024 update and 2026 review) 'Filtering and monitoring standards for schools and colleges'
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2023) 'Teaching online safety in school'
- Online safety Act 2023
- DfE Mobile Phones in schools 2024, updated 2026 guidance

2. **Roles and responsibilities**

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place across both schools
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Executive Headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

- Working with the DSL and ICT technicians to conduct light-touch reviews of this policy.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the SENCO, Computer lead and ICT technicians.

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

- Ensuring safeguarding is considered in the school's approach to remote learning.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.

- Understanding the filtering and monitoring processes in place at the school.

- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.

- Implementing appropriate security measures as directed by the headteacher.

- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

- Working with the DSL and Executive Headteacher to conduct light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Online safety teaching includes:

- Online radicalisation and prevent-related risks.
- Media literacy: how online content is created, curated, monetised and manipulated, and how to critically evaluate online information
- Understanding AI, deepfakes and synthetic media.

Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. **Managing online safety**

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Executive Headteacher has overall responsibility for the school's approach to online safety, with support from DSL's, the Computer lead and ICT technicians. The Executive Headteacher / DSL / DDSL's should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Our Internet access provides a service designed for pupils, including a "firewall" filtering and monitoring system through SWGFL; intended to prevent access to material inappropriate for children.
- Children using the Internet will usually be working in the classroom on laptops or iPads and will always be supervised by an adult.
- Staff will aim to check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- If staff or pupils discover an unsuitable site, it will be reported to the Class Teacher and then Computing Leader or IT Support Technician who will ensure that it is subsequently blocked.
- Staff will be particularly vigilant when pupils are undertaking their own research and will check that the children are following the agreed home/school agreement.
- Pupils will have access to information from relevant outside agencies.
- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum and within whole school assemblies.
- Assemblies / Computer lessons are conducted on the topic of remaining safe online

“In line with the Online Safety Act 2023, which came into force in stages during 2025, pupils, staff and parents are educated on platform duties relating to:

- Protection from illegal content (from March 2025)
- Protection from harmful content to children (from July 2025)
- Age assurance requirements for harmful content
- We teach pupils how to report inappropriate or illegal content and how platforms must respond under the law.”

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member’s online behaviour are reported to the Executive Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Executive headteacher, it is reported to the Chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Inclusion team and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Executive Headteacher contacts the police.

4. **Cyberbullying**

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying and Hate Policy.

5. **Child-on-child sexual abuse and harassment**

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

For further information refer to the Federations Safeguarding and Child Protection Policy.

6. **Online safety training for staff**

The Executive Headteacher / DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and

exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

7. **Online safety and the curriculum**

Online Safety incorporates Internet Technology and electronic communications such as mobile phones and other wireless technology. Technology is constantly changing at home and in the community; its impact on the lives of individuals continues to grow, therefore, it is essential to educate children about the benefits and risks of using new technology.

At the 'Forest of Dean Community Schools Federation', online safety is embedded throughout the curriculum and pupils will be taught about online safety as part of the National curriculum for computing. It will also be addressed in the following subjects:

- PHSE
- Relationships and Health Education
- Online Safety / Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- Using technology safely and respectfully, keeping personal information private
- Recognise acceptable and unacceptable online behaviour
- Identify where to go for help if they have concerns about online content or contact
- Identify a range of ways to support concerns about online content and contact

The DSL / DDSL's will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and pupils considered vulnerable.

Class teachers will aim to review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Executive headteacher and DSL will decide when it is

appropriate to invite external groups into school and ensure the visitors selected are appropriate.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

8. **Use of technology in the classroom**

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will aim to review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

9. **Use of smart technology**

The school complies with DfE 2024/26 guidance expecting schools to operate a mobile-phone-free environment by default. Mobile phones must be handed in on arrival. Smart watches may be worn only with restricted functionality.

10. **Educating parents and carers**

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be signposted to this policy with the attached copy of the Acceptable Use Agreement.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' assemblies delivered by outside agencies e.g. police, staff and pupils

- Information in newsletters / school websites
- Online resources

11. **Filtering and monitoring online activity**

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Executive Headteacher will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

"Our filtering and monitoring meets and is reviewed against the DfE 2024/26 Filtering & Monitoring Standards, including:

- Real-time scanning for harmful content, including AI-generated material (deepfakes, synthetic sexual content) [saferinternet.org.uk]
- Mandatory blocking of illegal content, which cannot be disabled under any circumstances [saferinternet.org.uk]
- Annual technical and safeguarding review, with formal reporting to governors and SLT, and evidence retained for Ofsted [gov.uk]
- Regular test checks, alert monitoring logs and rapid response workflows
- Filtering/monitoring of BYOD devices to the same standard as school devices [saferinternet.org.uk]

12. **Emails**

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Children's personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

13. **Social networking**

While on school premises, the use of social media by staff and pupils is not allowed.

14. **The school website**

The Executive Headteacher, Staff and Administrators are all responsible for the content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website will be checked at least annually by Governors and external reviews will be commissioned.

15. **Use of devices**

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary.

16. **Monitoring and review**

The governing board, Executive Headteacher and DSL will review this policy every two years.

Any changes made to this policy are communicated to all members of the school community.

17. **Links to other policies:**

- Safeguarding and Child Protection
- Health and Safety Policy
- Confidentiality
- Behaviour, Rewards and Sanctions
- Special Educational Needs and disabilities
- Staff code of conduct
- Whistleblowing
- Allegations against staff
- Anti-Bullying and Hate

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and their parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: EYFS / KS1 – TO BE SHARED AS PART OF THE COMPUTING CURRICULUM. (INCLUDED IN STARTER PACK FOR PARENTS)
When I use the school's ICT systems (like computers / tablets) and get onto the internet in school I will: Ask a teacher or adult if I can do so before using them Only use websites that a teacher or adult has told me or allowed me to use Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends Use school computers for school work only I will be kind to others and not upset or be rude to them Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly Only use the username and password I have been given Try my hardest to remember my username and password Never share my password with anyone, including my friends. Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer Save my work on the school network Check with my teacher before I print anything Log off or shut down a computer when I have finished using it Not bring a mobile phone or smart watch into school

Appendix 2: KS2, acceptable use agreement (pupils and their parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: KS2 – TO BE SHARED AS PART OF THE COMPUTING CURRICULUM.

(INCLUDED IN STARTER PACK FOR PARENTS)

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers / tablets) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer / tablet when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, clubs or other activities organised by the school and will hand it in to my class teacher at the start of the school day so it can go to the school office.

If I bring a smart watch into school:

- I will not use it during lessons, clubs or other activities organised by the school, will not get distracted by it or use it to make recording, take photos or receive or send messages / memes.

I know that the school can monitor the websites I visit and that there will be consequences if I don't follow the rules to keep me safe.

Appendix 3: acceptable use agreement (Given to parents as part of a starter pack)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS / CARERS
I will support the school to keep my child safe online. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the Internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet and using mobile technologies. I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy. I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's online safety. I will support the school by agreeing not to post negative comments / blogs on social media sites including Facebook/What App. Any concerns / complaints will be made in line with the school's complaints policy. I understand that posting complaints or defamatory statuses about the school, its pupils, staff or fellow parents can negatively affect the school. As such, the school has the right to request any damaging material to be removed. I understand that it is not appropriate to attempt to follow or friend request any member of staff on social media. I understand that parents can join class online chats with other parents, but these are to support the school not to slander or complain on. If my child in in the juniors I will remind them about the rules and expectations for mobile phones and smart watches. If my child breaks these rules, I understand the items may be banned.