



FOXWOOD ACADEMY E-SAFETY POLICY

Committee/Person Responsible for Policy:	E-Safety Coordinator / Headteacher/SLT/GB
Date Approved by HT/SLT:	5th January 2026
Next Review Due:	January 2027

1. Aims

Working and learning online are integral to Foxwood Academy's activities. We recognise and celebrate the role of the Internet in enhancing our work and contributing to pupil outcomes. However, we acknowledge the associated risks and are committed to doing everything possible to eliminate or mitigate these dangers.

This policy applies to all members of the Foxwood Academy community (including staff, pupils, volunteers, parents/carers, and visitors) who have access to and use Foxwood's ICT systems, both in and out of the school.

The Headteacher is empowered to reasonably regulate the behaviour of pupils when they are off the school site, and staff are empowered to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy that may occur outside of Foxwood Academy but are still linked to membership of the school. Such incidents will be addressed under this policy and associated behavioural expectations. Parents/carers will be informed of concerns via telephone or letter as appropriate.

Foxwood Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online.

- Deliver an effective approach to online safety, empowering the whole school community in the safe use of technology, including mobile and smart devices (e.g., ‘mobile phones’).
- Establish clear mechanisms to identify, intervene, and escalate incidents where appropriate.
- Key Categories of Risk Our approach to online safety addresses the following categories:
 - Content: Exposure to harmful content (e.g., pornography, fake news, racism, self-harm, extremism).
 - Contact: Harmful online interactions, including grooming, exploitation, or commercial advertising.
 - Conduct: Personal behaviours online that may harm others (e.g., bullying, sharing explicit content).
 - Commerce: Risks from online gambling, scams, and phishing.

2. Legislation and Guidance

This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying, including cyber-bullying

It also incorporates the DfE’s guidance on protecting children from radicalisation and existing legislation, including:

- The Education Act 1996 (as amended)
- The Education and Inspections Act 2006
- The Equality Act 2010
- The Education Act 2011, empowering teachers to search for and delete inappropriate materials on pupils’ devices when there is ‘good reason.’

Additionally, this policy aligns with the National Curriculum computing programmes of study and Foxwood Academy’s specific operational guidelines.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board of Foxwood Academy holds overall responsibility for monitoring and implementing this policy, ensuring the Headteacher is held accountable for its application.

The governing board will:

- Ensure all staff undergo online safety training as part of child protection and safeguarding training.

- Provide staff with regular updates on online safety, at least annually, via emails, bulletins, or staff meetings.
- Coordinate regular meetings with relevant staff to review online safety training needs and monitor logs provided by the designated safeguarding lead (DSL).
- Ensure children are taught how to keep themselves safe online.
- Ensure appropriate filtering and monitoring systems are in place on school devices and networks, and review their effectiveness annually.

The board will:

- Assign responsibilities to manage filtering and monitoring systems.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Develop effective monitoring strategies to meet safeguarding needs.

All governors will:

- Read and understand this policy.
- Adhere to the acceptable use terms for school ICT systems and the Internet.
- Embed online safety as a central theme in safeguarding and related procedures.
- Ensure that safeguarding teaching is adapted to meet the needs of vulnerable children, victims of abuse, or pupils with special educational needs and/or disabilities (SEND).

3.2 The Headteacher

The Headteacher is responsible for ensuring that all staff understand this policy and that it is consistently implemented throughout Foxwood Academy. The Headteacher is the e-safety coordinator at Foxwood.

Headteacher and Senior Leaders:

- The Headteacher ensures the safety of all members of the Foxwood community, including online safety.
- The Headteacher and senior leaders ensure relevant staff receive appropriate training and development to fulfil their e-safety roles and train other colleagues.
- The Headteacher and senior leaders maintain a system for logging and reviewing e-safety incidents within the school.
- The senior leadership team (SLT) at Foxwood Academy reviews and monitors e-safety incidents and is prepared to follow procedures in the event of serious allegations involving e-safety and staff.

Designated Member of SLT for E-Safety Responsibilities:

- Manage day-to-day e-safety issues and oversee sanctions for breaches of e-safety rules.
- Ensure all staff are familiar with procedures to follow during e-safety incidents.
- Provide training and support to staff on e-safety matters.
- Liaise with the Local Authority Designated Officer (LADO) or Police as necessary.
- Collaborate with IT staff and the safeguarding lead to resolve e-safety issues.

- Keep abreast of current e-safety guidance via organisations like CEOP, Childnet, UK Safer Internet Centre, and Prevent Radicalisation.

3.3 The Designated Safeguarding Lead (DSL)

Details of Foxwood Academy's DSL (and deputies) are outlined in the school's safeguarding policy. The DSL has lead responsibility for online safety, including:

- Supporting the Headteacher in ensuring staff understand and implement this policy.
- Collaborating with the Headteacher and governing board to review and update policies annually.
- Leading the understanding of filtering and monitoring systems for the school's ICT infrastructure.
- Managing e-safety incidents in line with the safeguarding policy and logging incidents appropriately.
- Addressing cyber-bullying incidents per the school's behaviour policy.
- Providing regular e-safety updates to staff, at least annually, as part of safeguarding updates.
- Undertaking risk assessments to reflect the online risks children face.
- Being trained in e-safety issues and understanding risks related to:
 - Sharing personal data.
 - Accessing illegal/inappropriate materials.
 - Grooming and inappropriate online contact.
 - Cyber-bullying.

3.4 IT Management and Technical Staff

Foxwood's IT team is responsible for:

- Maintaining effective filtering and monitoring systems on all school devices and networks.
- Conducting regular checks and updating safety mechanisms to protect against viruses, malware, and inappropriate content.
- Logging and addressing e-safety incidents according to the policy.
- Preventing access to potentially dangerous sites and blocking harmful downloads.

3.5 All Staff and Volunteers

All staff, including contractors, agency staff, and volunteers, are responsible for:

- Maintaining a thorough understanding of this policy and implementing it consistently.
- Adhering to Foxwood Academy's acceptable use policies for ICT systems.
- Reporting e-safety incidents to the DSL/E-Safety coordinator and ensuring they are logged and addressed appropriately.
- Embedding e-safety principles in curriculum and extracurricular activities.
- Monitoring ICT activity and addressing misuse of mobile phones, cameras, and other devices.

- Ensuring students are directed to appropriate, pre-checked online resources.
- Addressing all concerns about sexual violence or harassment, online or offline, while maintaining an attitude of “it could happen here.”
- Using social media appropriately, obtaining Headteacher approval before setting up resources like blogs, and ensuring such platforms are private and moderated.

3.6 Parents/Carers

Parents and carers play a critical role in helping their children understand the importance of using the internet and mobile devices safely and appropriately. Research shows that many parents may not fully understand online risks or the technology their children use. Foxwood Academy is committed to supporting parents/carers in this area through regular communications and resources provided via the school’s website.

Parents and carers are responsible for:

- Supporting and endorsing the Foxwood Academy E-Safety Policy.
- Accessing the school website in line with the Acceptable Use Policy.
- Notifying staff or the Headteacher of any concerns or queries regarding this policy.

For additional support, parents/carers can refer to:

- UK Safer Internet Centre – What are the issues?
- Childnet – Hot topics and Parent resource sheets
- The National Online Safety App.

3.7 Visitors and Members of the Community

Visitors and community members using Foxwood Academy’s ICT systems or internet will be made aware of this policy where relevant and are expected to comply with it. They may also be required to agree to the acceptable use terms.

4. Educating Pupils About Online Safety

Foxwood Academy integrates e-safety education into the curriculum to empower pupils to use technology safely and responsibly.

Approaches include:

- A planned e-safety program delivered through the ICT curriculum.
- Reinforcing key e-safety messages during assemblies and PSHE lessons, including topics on British Values and radicalisation.
- Encouraging pupils to critically assess the material they access online and validate its accuracy.
- Promoting safe and responsible ICT, internet, and mobile device use both in and outside school.
- Teaching pupils to respect copyright and properly acknowledge sources.

Primary Provision

In KS1, pupils learn:

- o Safe and respectful technology use.
- o How to keep personal information private.
- o Where to seek help with online concerns.

In KS2, pupils learn:

- o Safe and responsible technology use.
- o Recognising acceptable and unacceptable behaviours online.
- o Reporting concerns about content and contact.

Secondary Provision:

In KS3 and KS4, pupils are taught:

- o To use technology safely, respectfully, and securely, including protecting their privacy and identity.
- o How to report inappropriate content, contact, and conduct.
- o Understanding online risks, rights, and responsibilities.
- o The importance of consent in online interactions and the risks of sharing personal material.

Where necessary, e-safety education is adapted to meet the needs of vulnerable children, victims of abuse, or pupils with SEND.

More information including E-Safety and Computing Key Stage End Points are available on the Academy website under 'Curriculum'.

5. Educating Parents/Carers About Online Safety

Foxwood Academy engages parents/carers by:

- Raising awareness of internet safety through letters, website updates, and parents' evenings.
- Explaining the school's filtering and monitoring systems.
- Clarifying what pupils are asked to do online and how parents/carers can support safe internet use at home.
- Concerns about online safety or this policy should be directed to the Headteacher or DS or via the direct link on the school's website.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying involves using online platforms such as social media, messaging apps, or gaming sites to repeatedly and intentionally harm another person or group where there is an imbalance of power.

6.2 Preventing and Addressing Cyber-Bullying

Foxwood Academy will:

- Educate pupils on recognising, reporting, and preventing cyber-bullying.
- Provide resources and curriculum links, such as PSHE education, to address cyber-bullying.
- Support pupils and parents/carers with information about recognising signs of cyber-bullying and responding appropriately.

If incidents occur, the school will follow its behaviour policy to address and contain the issue. The DSL may involve external services or law enforcement when necessary.

6.3 Examining Electronic Devices

Foxwood Academy staff may examine or confiscate electronic devices under specific conditions, such as:

- Risk to staff or pupils.
- Violation of school rules.
- Suspected involvement in an offence.

Staff will follow appropriate safeguarding and privacy procedures, including consulting the DSL or Headteacher for guidance. Devices containing illegal content will be handed to the police.

6.4 Artificial Intelligence (AI)

Generative AI tools, such as ChatGPT or Google Bard, offer educational benefits but may also pose risks. For example, they can be misused to create 'deepfake' content or facilitate cyber-bullying.

Foxwood Academy will address AI misuse in line with its anti-bullying and behaviour policies. Staff must assess risks before integrating AI tools into school activities.

7. Acceptable Use of the Internet in School

All users of Foxwood Academy's ICT systems must adhere to the Acceptable Use Policy. The school monitors online activity and restricts access to harmful content through filtering systems.

8. Pupils Using Mobile Devices in School

Mobile device use must comply with Foxwood Academy's acceptable use guidelines. Breaches may lead to disciplinary action, including device confiscation, per the behaviour policy.

9. Staff Using Work Devices Outside School

Staff must secure work devices by:

- Using strong passwords and encryption.
- Locking devices when inactive.
- Avoiding personal use or sharing with others.
- Keeping software up-to-date.

Concerns about device security should be reported to the school's IT lead.

10. How the School Will Respond to Misuse

Misuse of Foxwood Academy's ICT systems is addressed according to its behaviour and staff disciplinary policies. Incidents involving illegal activity are reported to the police as required.

11. Training

All new staff members at Foxwood Academy will receive training on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

Ongoing Training:

- All staff will participate in refresher training at least annually as part of safeguarding updates. Additional updates will be provided via emails, bulletins, or staff meetings.

Training will emphasize:

- The role of technology in safeguarding and the risks of online abuse.
- Peer-to-peer online abuse, including:
- Abusive, threatening, and misogynistic messages.
- Non-consensual sharing of indecent images or videos.
- Sharing unwanted abusive images or pornography.
- The intersection of physical abuse and online activity, including sexual violence.

Training Objectives:

- Help staff identify signs and symptoms of online abuse.
- Equip staff to educate pupils on online risks and how to make informed decisions.
- Enable staff to promote long-term online safety and well-being among pupils.

Designated Safeguarding Lead (DSL):

- The DSL and deputies will undertake child protection and online safety training every two years, with annual updates on current issues and best practices.
- Governors will receive training on internet safety as part of their safeguarding responsibilities.
- Volunteers will be provided with relevant training and updates, where applicable.

More information is detailed in the Foxwood Academy Child Protection and Safeguarding Policy.

12. Monitoring Arrangements

The DSL logs all behaviour and safeguarding issues related to online safety using Foxwood's electronic safeguarding system.

The policy will be reviewed annually by Foxwood Academy's safeguarding and IT leads, supported by an annual risk assessment to reflect emerging online risks.

13. Use of Digital and Video Images

13.1 Digital Imaging and Learning

Foxwood Academy recognises the educational benefits of digital imaging but also highlights the potential risks associated with sharing and posting digital content online.

13.2 Risk Mitigation:

Staff must educate pupils about the risks of taking, sharing, and publishing images online.

Staff may use digital/video images for educational purposes but only with school equipment. Personal devices must not be used.

Images must be stored securely on Foxwood systems, not personal devices.

Care must be taken to ensure pupils are appropriately dressed and engaged in appropriate activities when images are captured.

Guidelines:

- Pupils must not share images of others without permission.
- Parental consent will be obtained before publishing pupil images on the school website.
- Downloading, copying, or printing images from the internet must comply with copyright laws.

14. GDPR and Prevent

14.1 GDPR Compliance

Foxwood Academy adheres to GDPR requirements for recording, processing, and transferring personal data. Please refer to the school's GDPR policy for more details.

14.2 Communications

Staff and pupils should be aware that email communications may be monitored. Any email that makes users feel uncomfortable, or contains offensive or bullying content, must be reported immediately to SLT.

Staff must only use official school systems for communication with students or parents. Personal accounts must not be used.

Pupils will be taught email safety, including how to handle inappropriate messages.

14.3 Prevent Duty

Foxwood Academy ensures children are safeguarded from radicalisation and extremist material online. While robust filtering is in place, staff must remain vigilant regarding the risks posed by radicalisation groups.

15. Responding to Incidents of Misuse

15.1 Illegal Activity

If misuse involves illegal activity, such as:

- Child sexual abuse images.
- Racist or obscene material.
- Radicalization of others.

The Headteacher must be informed immediately. Relevant authorities, including law enforcement, will be notified. All steps taken will be logged and reported by the safeguarding lead.

16. Links with Other Policies

This E-Safety Policy is closely connected to the following Foxwood Academy policies and procedures:

- Child Protection and Safeguarding Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy
- Other relevant policies relating to safeguarding and e-safety.