



Glenmoor & Winton Academies

High Achievement – High Standards

Part of United Learning

Online Safety Policy

1. Policy Statement

Glenmoor and Winton Academies are committed to safeguarding and promoting the welfare of all students, including when they are accessing digital technologies.

Online safety is a fundamental aspect of safeguarding. We recognise that while technology offers significant educational and social benefits, it also presents risks that must be carefully managed.

This policy sets out how the academies will:

- Protect students and staff online
- Educate users about safe and responsible use
- Respond effectively to online safety concerns
- Meet statutory requirements, including Keeping Children Safe in Education 2025 (KCSIE 2025)

This policy should be read in conjunction with the Safeguarding and Child Protection Policy, which includes online safety as a core component of safeguarding.

2. Scope

This policy applies to all members of the school community, including:

- Students
- Staff (teaching and support)
- Governors
- Parents and carers
- Volunteers, visitors and contractors

It applies to:

- Use of academy devices and networks
- Personal devices (including BYOD)
- Off-site and remote use where individuals access academy systems or represent the academies

3. Aims

The academies aim to:

- Safeguard students from online harm
- Promote safe, responsible and respectful online behaviour
- Ensure robust systems for filtering, monitoring and reporting
- Provide effective education on online safety
- Respond promptly and effectively to concerns
- Comply fully with statutory safeguarding and data protection requirements

4. Understanding Online Risk

Online risks are understood under the four key areas:

- Content: Exposure to harmful, illegal or inappropriate material
- Contact: Harmful interaction with others (e.g. grooming, exploitation)
- Conduct: Behaviour that increases risk (e.g. bullying, sharing images)
- Commerce: Financial risks such as scams and fraud

The academies recognise specific online safeguarding risks, including:

- Cyberbullying
- Online grooming and child exploitation
- Child-on-child abuse online
- Sharing of nude or semi-nude images
- Exposure to violent, harmful, or extremist content
- Misinformation and disinformation
- Online radicalisation
- Gaming-related risks
- Risks associated with live streaming and social media platforms

5. Emerging Risks and Artificial Intelligence

The academies recognise the increasing risks associated with emerging technologies, including artificial intelligence (AI).

These include:

- Deepfakes and manipulated media
- Misinformation and disinformation
- Misuse of generative AI tools
- Loss of privacy or data misuse

Staff and students are expected to use AI responsibly in line with Acceptable Use Policies. Staff are supported to understand emerging risks and adapt safeguarding responses accordingly.

6. Roles and Responsibilities

Governing Body

- Ensure statutory safeguarding duties are met
- Review online safety provision annually
- Provide strategic oversight and challenge

Principal

- Overall accountability for online safety
- Ensure effective systems, training and policy implementation

Designated Safeguarding Lead (DSL)

- Lead responsibility for online safety
- Manage and respond to incidents
- Maintain safeguarding records
- Work with external agencies where required
- Ensure staff training is up to date

ICT Lead

- Implement and maintain filtering and monitoring systems
- Ensure cybersecurity is robust
- Work closely with the DSL on safeguarding risks

Staff

- Model safe and professional behaviour
- Deliver online safety education
- Supervise students appropriately
- Report concerns immediately

Students

- Follow Acceptable Use Policies
- Use technology responsibly
- Report concerns

Parents/Carers

- Support safe use of technology at home
- Engage with school guidance and communication

7. Education and Training

Online safety education is delivered through:

- PSHE and Relationships/Health Education
- Curriculum subjects
- Assemblies and enrichment activities

The curriculum equips students to:

- Understand online risks
- Make safe choices

- Report concerns
- Think critically about online content

Training

- Staff receive annual safeguarding and online safety training
- DSLs receive enhanced training
- Governors receive safeguarding updates

8. Filtering, Monitoring and Cybersecurity

The academies maintain effective filtering and monitoring systems to safeguard users.

We will:

- Regularly review filtering and monitoring systems (at least annually)
- Ensure systems are appropriate to risk and age range
- Clearly define roles and responsibilities for monitoring
- Ensure the DSL receives and responds to safeguarding alerts
- Ensure leaders and governors understand systems and risks

Filtering and monitoring arrangements are informed by risk assessment and follow DfE standards.

Cybersecurity

We maintain robust cybersecurity measures, including:

- Secure networks and password protocols
- Regular updates and patching
- Staff awareness of phishing and scams

9. Acceptable Use of Technology

This policy is supported by Acceptable Use Policies (AUPs) for:

- Staff
- Students
- Visitors

These outline expectations for safe and appropriate use of:

- Internet and networks
- Devices
- Communication systems
- Social media

10. Use of Images, Media and Social Platforms

The academies will:

- Obtain appropriate consent for images and media
- Ensure safe storage and use of images
- Require staff to use academy-approved systems and devices
- Maintain professional boundaries in all online interactions

11. Data Protection and Privacy

The academies comply with:

- UK GDPR
- Data Protection Act 2018

We ensure:

- Secure handling of personal data
- Use of encrypted and password-protected systems
- Staff training on data protection

12. Responding to Online Safety Incidents

All concerns must be reported immediately to the DSL.

The DSL will:

- Assess and record incidents
- Take appropriate safeguarding action
- Involve parents/carers where appropriate
- Refer to external agencies when necessary

This may include:

- Police
- Children's social care
- Local Authority Designated Officer (LADO)
- Prevent / Channel panels

Appropriate sanctions will be applied in line with the Behaviour Policy.

13. Mobile Devices and Off-Site Use

This policy applies to:

- Personal devices used on site
- Remote learning environments

- Off-site use of academy systems

Expectations for mobile phones and personal devices are set out in the Behaviour and AUP policies.

14. Monitoring, Evaluation and Review

The academies will:

- Monitor patterns of incidents and concerns
- Review filtering and monitoring effectiveness
- Gather feedback from students and staff
- Report regularly to senior leaders and governors

This policy is reviewed:

- Annually
- Or sooner in response to changes in guidance or emerging risks

15. Links to Other Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Policies
- Anti-Bullying Policy

16. Complaints and Concerns

Concerns about online safety should be raised:

1. With a member of staff or the DSL
2. Through safeguarding systems
3. Via the Complaints Policy if unresolved

All concerns are taken seriously and addressed promptly.

Prepared:	June 2026
Ratified by Governors:	June 2026
Next Review Date:	July 2027

