



Onside Education

E-Safety Policy

Issue Date: Sept 2025

Review Date Sept 2026

Onside Education

Online Safety, Filtering and Monitoring Policy

September 2025

1. Policy Statement

Onside Education recognises that online safety is a safeguarding issue and forms an integral part of our wider safeguarding responsibilities.

The provision is committed to creating a culture where pupils, staff, volunteers and visitors can use technology safely, responsibly and appropriately.

Online safety risks are managed through:

- Education
- Filtering
- Monitoring
- Safeguarding procedures
- Staff training
- Acceptable use agreements
- Clear reporting processes

This policy complies with:

- Keeping Children Safe in Education (KCSIE) 2025
- Independent School Standards
- Data Protection Act 2018
- UK GDPR
- Working Together to Safeguard Children

2. Scope

This policy applies to:

- Pupils
- Staff
- Volunteers
- Proprietors
- Contractors
- Visitors
- Any device used to access provision systems or networks

This includes:

- Onsite learning
- Offsite activities
- Educational visits
- Remote learning
- School-owned devices
- Personal devices where authorised

3. Online Safety Responsibilities

Proprietor

The Proprietor will:

- Ensure appropriate filtering and monitoring systems are in place;
- Receive assurance regarding the effectiveness of Smoothwall Filter and Smoothwall Monitor;
- Review filtering and monitoring arrangements annually;
- Ensure online safety forms part of safeguarding governance and risk management.

Designated Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety, filtering and monitoring and will:

- Review Smoothwall monitoring alerts and reports;
- Ensure safeguarding concerns are acted upon promptly;
- Maintain records of online safety incidents;
- Review filtering and monitoring effectiveness at least annually;
- Report significant online safety concerns to the Proprietor;
- Ensure staff receive appropriate online safety and filtering/monitoring awareness training.

IT Provider (Smoothwall)

The IT provider will:

- Maintain filtering systems.
- Maintain monitoring systems.
- Generate alerts and reports.
- Support incident investigations.
- Conduct regular system reviews.

Staff

All staff must:

- Promote safe online behaviour.

- Report concerns immediately.
- Follow acceptable use requirements.
- Complete online safety training.

4. The Four Areas of Online Risk

Online safety education will address the four categories identified by KCSIE:

Content

Exposure to harmful, illegal or inappropriate content including:

- Extremism
- Violence
- Pornography
- Self-harm content
- Hate content
- Misinformation

Contact

Risks from interaction with others including:

- Grooming
- Exploitation
- Radicalisation
- Coercion
- Online predators

Conduct

Behaviour online including:

- Cyberbullying
- Sharing harmful content
- Online abuse
- Harassment
- Peer-on-peer abuse

Commerce

Risks relating to:

- Fraud
- Scams

- Gambling
- Financial exploitation
- Inappropriate advertising

5. Filtering and Monitoring

Onside Education uses Smoothwall Filter and Smoothwall Monitor to support its statutory safeguarding responsibilities and comply with the Department for Education's filtering and monitoring standards and Keeping Children Safe in Education (KCSIE) 2025.

Although pupil internet access is limited and generally restricted to supervised educational activities such as Esports provision, Onside Education maintains appropriate filtering and monitoring arrangements across its network and devices.

Filtering and monitoring arrangements apply to:

- Staff devices;
- Provision-owned devices;
- Any devices used by pupils for authorised educational activities;
- Esports provision where internet connectivity is required;
- Any future educational technology introduced within the provision.

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety and works with Smoothwall and the provision's IT support arrangements to ensure filtering and monitoring systems remain effective, proportionate and appropriate to the needs of the provision.

Smoothwall Filter is used to:

- Block access to harmful, illegal or inappropriate content;
- Restrict access to unsuitable websites and services;
- Support safeguarding and online safety requirements;
- Provide age-appropriate access to online resources.

Smoothwall Monitor is used to:

- Identify potential safeguarding concerns;
- Generate alerts relating to self-harm, suicide ideation, bullying, exploitation, extremism, violence and other online risks;
- Support early intervention and safeguarding responses;
- Provide monitoring information to authorised safeguarding staff.

All monitoring alerts will be reviewed by authorised staff and escalated in accordance with the Safeguarding and Child Protection Policy.

Filtering and monitoring arrangements will be formally reviewed at least annually by the DSL and Proprietor to ensure systems remain effective and continue to meet statutory requirements.

6. Online Monitoring Alerts

Alerts generated by monitoring systems may relate to:

- Self-harm
- Suicide ideation
- Child sexual abuse material
- Extremism
- Violence
- Grooming concerns
- Bullying
- Safeguarding disclosures

All alerts will be reviewed promptly and escalated according to safeguarding procedures.

Actions taken will be recorded.

7. Use of Devices

Pupil access to technology will be determined according to age, need, curriculum requirements and risk assessment.

Where pupils access devices:

- Appropriate filtering and monitoring will apply.
- Supervision arrangements will be in place.
- Acceptable use expectations will be explained.

Where mobile phones are prohibited, arrangements will be managed in accordance with the Mobile Phone Policy.

Esports Provision

Where internet access is required for Esports activities:

- Pupils will be supervised by staff.
- Access will be restricted to approved platforms.
- Online interactions will be monitored where reasonably practicable.
- Behaviour expectations remain consistent with the Behaviour Policy.
- Safeguarding concerns arising from online activity will be managed through safeguarding procedures.

Onside Education operates a highly restricted technology environment. Pupils do not have routine access to Wi-Fi, email accounts or internet-enabled devices during the school day. Internet access is generally limited to supervised educational activities, including Esports provision and authorised curriculum activities, with appropriate filtering and monitoring in place.

8. Remote Learning

Where remote learning takes place:

- Approved platforms will be used.
- Staff will use professional accounts only.
- Sessions will be appropriately supervised.
- Safeguarding procedures remain fully applicable.

Online learning arrangements will follow safeguarding and data protection requirements.

9. Artificial Intelligence (AI)

The use of AI tools presents both opportunities and risks.

Staff and pupils must:

- Use AI responsibly.
- Verify information generated by AI systems.
- Avoid sharing personal information with AI tools.
- Follow data protection requirements.

AI must not be used to:

- Create harmful content.
- Facilitate cheating.
- Generate inappropriate images.
- Circumvent safeguarding controls.

10. Cyberbullying and Online Abuse

Cyberbullying is treated as a safeguarding and behaviour concern.

Examples include:

- Online harassment.
- Threatening messages.
- Sharing images without consent.
- Exclusion from online groups.
- Impersonation.

Incidents will be managed through:

- Behaviour procedures.
- Safeguarding procedures.
- Anti-Bullying arrangements.

11. Child-on-Child Online Abuse

Online abuse between children may include:

- Sexual harassment.
- Harmful sexual behaviour.
- Coercion.
- Image sharing.
- Exploitation.

All incidents will be treated seriously and managed in accordance with safeguarding procedures.

12. Nude and Semi-Nude Images

The sharing of nude or semi-nude images is a safeguarding concern.

Staff must:

- Never view or share images unnecessarily.
- Report concerns immediately to the DSL.
- Follow national guidance and safeguarding procedures.
- Preserve evidence where appropriate.

The DSL will determine whether external agencies should be involved.

13. Social Media

Staff and pupils must use social media responsibly.

Staff must not:

- Contact pupils using personal accounts.
- Share confidential information.
- Blur professional boundaries.

Online conduct outside work may affect suitability to work with children.

14. Data Protection and Privacy

Monitoring arrangements operate in accordance with:

- UK GDPR
- Data Protection Act 2018
- Human Rights Act

Personal staff devices will not be searched routinely.

Where examination of a device is necessary:

- The action must be lawful.

- The action must be proportionate.
- The reason must be recorded.
- Relevant safeguarding or disciplinary procedures will be followed.

15. Acceptable Use Agreements

All staff and pupils will sign appropriate Acceptable Use Agreements covering:

- Device use.
- Internet access.
- Online conduct.
- Password security.
- Reporting concerns.

16. Online Safety Education

Pupils will receive online safety education through:

- PSHE
- Safeguarding education
- Digital literacy activities
- Individual interventions where required

Staff will receive:

- Induction training
- Annual safeguarding updates
- Online safety updates
- Filtering and monitoring awareness training

17. Incident Reporting

Online safety concerns must be reported immediately to the DSL.

Concerns may include:

- Harmful content.
- Online abuse.
- Cyberbullying.
- Grooming concerns.
- Radicalisation concerns.
- Filtering failures.

All incidents will be recorded and reviewed.

Serious online safeguarding concerns may also require referral to Children's Services, the Police, the LADO or other relevant agencies in accordance with the Safeguarding and Child Protection Policy.

18. Monitoring and Review

The DSL and Proprietor will review:

- Online safety incidents.
- Filtering effectiveness.
- Monitoring effectiveness.
- Staff training needs.
- Emerging online risks.

This review will take place at least annually.

The annual review will include consideration of filtering and monitoring effectiveness, online safety incidents, emerging risks and any recommendations arising from Smoothwall reporting.

19. Related Policies

- Safeguarding and Child Protection Policy
- Mobile Phone Policy
- Behaviour Policy
- Anti-Bullying Policy
- Remote Education Policy
- Staff Code of Conduct
- Data Protection Policy
- Filtering and Monitoring Procedures

20. Review

This policy will be reviewed annually or sooner if:

- Legislation changes.
- KCSIE is updated.
- Significant incidents occur.
- Filtering and monitoring arrangements change.