



Joanna Gardner

ONLINE SAFETY



Projection Education

Online Safety Policy

September 2026

1. Purpose and Scope

This Online Safety Policy outlines how Projection Education promotes safe, responsible, and appropriate use of digital technology for all pupils, staff, and visitors. It applies to:

- All pupils attending Projection Education
- All staff, volunteers, and external professionals
- All devices used on site, including school-owned and personal tablets, phones, laptops, and gaming equipment
- All online activity taking place during the provision's operating hours or using Projection Education's network or equipment

Given the unique needs of our pupils — including those with SEND and those in care, this policy ensures that online safety is embedded into daily practice, supervision, and curriculum.

2. Our Online Safety Principles

Projection Education is committed to:

- Creating a safe digital environment for all pupils
- Teaching children to use technology responsibly
- Protecting vulnerable learners from online harm
- Ensuring staff understand their safeguarding responsibilities
- Working closely with parents, carers, and social workers
- Responding swiftly to concerns, incidents, or disclosures



Projection Education recognises the four online risk areas identified in Keeping Children Safe in Education (KCSIE): content, contact, conduct and commerce and Working Together to Safeguard Children. Online safety education, supervision, filtering, monitoring and incident response procedures are structured around these four areas and are tailored to pupils' age, developmental stage, SEND needs and individual vulnerabilities. This ensures that safeguarding measures remain proportionate, responsive and effective in meeting the diverse needs of all learners.

3. Understanding Our Pupils' Needs

Many of our pupils:

- Have SEND (including SEMH, ASD, ADHD, communication needs, and learning difficulties)
- Are looked-after children or have complex home circumstances
- Use gaming as a primary form of engagement
- Have regular access to tablets, phones, and screens
- Require 1:1 support at all times

These factors increase vulnerability to:

- Online grooming
- Cyberbullying
- Exposure to inappropriate content
- Online scams or exploitation
- Excessive screen time
- Unsafe gaming interactions
- Sharing personal information

Our approach is therefore highly supervised, personalised, and proactive.

4. Roles and Responsibilities

Online Safety Lead



The online safety lead is the proprietor, Mr Will Harvey with the overall responsibility for the duties of the senior leadership team.

wharvey@projection-edu.co.uk

Senior Leadership Team

- Ensures online safety is embedded in safeguarding practice
- Reviews and updates this policy annually
- Ensures staff receive regular training

Designated Safeguarding Lead (DSL)

- Leads responses to online safety concerns
- Maintains records of incidents
- Liaises with external agencies where needed
- Supports staff to manage online risks

Staff

- Supervise all pupil online activity
- Model safe and responsible digital behaviour
- Report concerns immediately to the DSL
- Follow filtering, monitoring, and device-use procedures

Parents/Carers/Social Workers

- Support safe use of technology at home
- Communicate concerns to the DSL
- Work collaboratively with the provision to safeguard pupils

Pupils

With support, pupils are encouraged to:

- Use technology respectfully
- Follow adult instructions
- Report anything that makes them uncomfortable

5. Supervision and Access Controls



1:1 Supervision

All pupils are supervised closely at all times, including during:

- Gaming
- Internet browsing
- Use of tablets
- Online learning activities

Filtering and Monitoring

Projection Education uses:

- Age-appropriate filtering to block harmful content
- Monitoring software to flag concerning activity
- Staff oversight to ensure safe use
- The Proprietor is accountable for ensuring that filtering and monitoring arrangements are in place. The DSL is responsible for reviewing safeguarding concerns arising from monitoring alerts. The proprietor will review the effectiveness of filtering and monitoring at least annually, and after any serious online safety incident. Staff will receive training on the school's filtering and monitoring arrangements at induction and through annual safeguarding updates.

Device Use

- Personal devices may only be used with staff permission
- Personal devices will only be searched, viewed or confiscated in line with the school's Searching, Screening and Confiscation procedures, safeguarding policy and staff code of conduct. Staff must not view, copy or forward suspected nude or semi-nude images; they must secure the device where necessary and refer immediately to the DSL.
- Pupils may not access social media unless part of a planned, supervised activity (subject to the social media laws implanted in Spring 2027)
- Online gaming is restricted to age-appropriate, pre-approved games

6. Gaming Safety

Given the popularity of gaming among our pupils, we ensure:



- Only PEGI-appropriate games are used
- Online chat functions are disabled where possible
- Pupils do not interact with strangers online
- Staff monitor all gameplay
- Gaming is used as a tool for engagement, social skills, and regulation

7. Teaching Online Safety

Online safety is taught through:

- PSHE sessions
- Online Safety assemblies
- 1:1 discussions
- Social stories
- Visual supports
- Modelling safe behaviour
- Reinforcing simple rules such as:
 - “Don’t share your name or address online”
 - “Tell an adult if something feels wrong”
 - “Only talk to people you know in real life”

Teaching is adapted to each child’s developmental level and SEND profile.

8. Managing Incidents and Concerns

Any online safety concern — including exposure to harmful content, cyberbullying, or unsafe online behaviour — is:

1. Reported immediately to the DSL
2. Recorded on the safeguarding system
3. Investigated and responded to
4. Shared with parents/carers/social workers where appropriate
5. Used to inform future risk assessments



Serious incidents may be referred to:

- Police
- Children's Social Care
- CEOP

9. Staff Training

All staff receive training on:

- Online risks for vulnerable children
- Gaming-related risks
- Grooming and exploitation
- Managing disclosures
- Safe supervision of devices

10. Data Protection and Privacy

Projection Education follows GDPR and data protection legislation.

We ensure:

- Personal data is stored securely
- Pupils do not share personal information online
- Staff use secure systems for communication and record-keeping

11. Remote Learning (if applicable. Please see separate remote learning policy)

If remote learning is used:

- Sessions are supervised
- Platforms are secure
- Staff follow safeguarding procedures
- Parents/carers are supported to maintain safe home environments

12. Policy Review



This policy is reviewed annually or sooner if:

- Legislation changes
- New risks emerge
- A significant incident occurs

Updated Jan 2026