E-Safety Policy
September 2025 (to be reviewed annually)

1. Purpose of This Policy

This ESafety Policy outlines how Reach for Inclusion protects children and young people when using digital technologies. It sets out expectations for safe and responsible use of the internet, electronic devices and communication systems, and explains how filtering, monitoring and supervision contribute to safeguarding practice.
This policy should be read alongside:

- Child Protection & Safeguarding Policy
- Behaviour and Anti-Bullying Policy
- Staff Code of Conduct
- Student Mobile Phone Policy
- Acceptable Use Agreements (Students, Staff and Visitors)

2. Safeguarding Commitment

Reach for Inclusion is committed to ensuring that all children and young people:

- Are protected from harm and risk when using digital technology
- Understand online risks and how to respond safely
- Are taught the knowledge and skills to stay safe online
- Have access to filtered, monitored and secure systems
- Know how to report concerns and feel confident to do so

Staff understand that online safety is part of statutory safeguarding duties and must be considered within all aspects of teaching, supervision and pastoral support.

3. Filtering and Monitoring Statement

3.1 Filtering

Reach for Inclusion uses robust, age-appropriate and regularly reviewed filtering systems to restrict access to harmful or inappropriate online content.
Filtering prevents access to:

- Extremism and radicalisation content
- Violence or hate-based material
- Pornography or sexualised content
- Gambling websites
- Illegal drug content and substance misuse promotion
- Self-harm or suicide content
- Malware, phishing, unsafe downloads or untrusted sources
- Gaming, streaming and social networks not permitted for student use

Filtering is applied across all student devices and the organisation's network, including Wi-Fi accessible areas.
The filtering system is reviewed at least annually or sooner if risks, technology or safeguarding circumstances change.

3.2 Monitoring

Monitoring is a critical safeguarding measure and operates across all school systems.
Reach for Inclusion carries out active and automated monitoring to:

- Detect unsafe, concerning or harmful online behaviour

- Identify early signs of online grooming, exploitation or bullying
- Prevent attempts to access inappropriate or dangerous material
- Support staff to take timely action
- Ensure compliance with the Acceptable Use Agreements
- Protect system integrity and prevent misuse

Monitoring includes:

- Web activity logs
- Keyword/phrase alerts relating to safeguarding risks
- Device usage reports
- Email and communication monitoring within school platforms
- Reports of attempts to bypass filters or use prohibited tools

Any monitoring concerns are reviewed by the Designated Safeguarding Lead (DSL) or a member of the safeguarding team in line with child protection procedures.

4. Education & Prevention

4.1 Online Safety Education

Reach provides regular, age-appropriate learning to support young people's understanding of online risk, including:

- Cyberbullying and respectful communication
- Digital footprint and privacy
- Safe use of social media and messaging apps
- Reporting concerns and accessing support

Online safety is embedded across the curriculum and revisited throughout the year.

4.2 Workshops and Specialist Sessions

Reach for Inclusion provides dedicated workshops focused on:

- Online safety and digital resilience
- Exploitation (criminal and sexual exploitation, grooming, county lines)
- Drugs and substance misuse**,** including how these topics are promoted online
- Healthy online relationships
- Managing peer pressure and harmful content online

These may be delivered by staff or external agencies with expertise in safeguarding.

5. Acceptable Use Expectations

All students, staff and visitors must follow the appropriate Acceptable Use Agreement**,** which outlines responsibilities for safe, lawful and respectful use of:

- Devices
- Internet access
- Social media platforms
- Communication systems
- Personal devices on-site

Breaches of acceptable use will be recorded and may trigger safeguarding intervention where necessary.

6. Reporting Concerns

Students, staff and parents are encouraged to report:

- Inappropriate online behaviour
- Harmful or unsafe content
- Cyberbullying

- Online threats or grooming
- Concerns about exploitation, drug use or risky behaviour

Reports can be made to any member of staff but must be forwarded promptly to the DSL**.** Monitoring alerts are reviewed by the safeguarding team and action is taken in line with the Child Protection Policy.

7. Roles and Responsibilities

Designated Safeguarding Lead (DSL)

- Oversees all aspects of online safety
- Reviews filtering/monitoring reports
- Responds to alerts and concerns
- Ensures staff training and student education

Staff

- Model safe, responsible behaviour online
- Supervise students during digital activities
- Report concerns without delay
- Teach or reinforce online safety principles

Students

- Follow the Acceptable Use Agreement
- Use technology responsibly and safely
- Report anything that makes them feel uncomfortable

8. Review of Policy

This policy will be reviewed annually**,** or sooner if:

- Legislation changes
- Technology changes
- A safeguarding incident indicates a need
- Monitoring or filtering reviews highlight emerging risks

Policy	E-Safety Policy
Date created	September 2023
Date Reviewed	September 2025
Date of Next Review	September 2026
Signed:	
Siobhan Williams	S Williams
Jo Garner	J. Garner