IT and E-Safety Policy

2025 - 2026

Date Approved: August 2022
Review Date: August 2025
Next Review Date: August 2026

REACH Learning Provision
6 and 7b Russell Place
Nottingham
NG1 5HJ
Office Number: 0115 6462127
Email Address: Admin@ReachLearningProvision.org

Approved by: Corrine Scott
Position: Head of Provision

Introduction

REACH Learning Provision recognises that digital technologies are integral to education, communication, and social development. While they provide significant benefits, they also present safeguarding risks that must be managed effectively.
This policy sets out how REACH ensures safe, responsible, and positive use of technology by students, staff, parents/carers, and visitors. It should be read alongside the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, and GDPR & Data Protection Policy.

This policy is guided by:

- *Keeping Children Safe in Education (KCSIE) 2025*
- DfE Filtering and Monitoring Standards (2023)
- The Prevent Duty (2015)
- The Children Act (1989/2004)

Purpose

The purpose of this policy is to:

- Safeguard all members of the REACH community online.
- Promote responsible and positive use of digital technology.
- Provide clear expectations for safe behaviour and role modelling.
- Identify risks and set out procedures for responding to incidents.
- Equip students with skills to evaluate online content and protect themselves.
- Ensure staff and parents/carers are supported to keep young people safe online.

Scope

This policy applies to:

- All staff, governors, volunteers, contractors, and visitors.
- All students on roll at REACH.
- Parents/carers engaging with the provision.

It covers use of provision ICT systems, personal devices used on site, and behaviour online that impacts REACH or its community.

Roles & Responsibilities

Staff

- Read, understand, and sign the Staff Acceptable Use Agreement (AUA).
- Use provision systems for all work-related communication.
- Report concerns or incidents to the DSL immediately.
- Model professional, safe behaviour online.
- Embed e-safety into the curriculum (e.g. ICT, PSHE).

Designated Safeguarding Lead (DSL)

- Ensure staff, students, and parents receive up-to-date training.
- Lead on incident response, referrals, and liaison with external agencies.
- Monitor trends in online safety risks (e.g. sexting, grooming, AI-generated abuse).
- Ensure compliance with statutory duties and annual policy review.

Students

- Sign and follow the Student Acceptable Use Agreement.
- Report concerns or inappropriate material to staff.
- Understand expectations for safe behaviour online and in the use of devices.
- Never share indecent or harmful images, engage in cyberbullying, or bypass security systems.

Parents/Carers

- Support REACH's e-safety messages at home.
- Monitor children's use of devices and social media.
- Attend workshops or guidance sessions where offered.
- Report concerns to the provision promptly.

Safe Use of Technology

Benefits

ICT and the internet enhance teaching and learning by:

- Providing access to worldwide resources, experts, and cultural experiences.
- Enabling interactive, individualised learning.
- Supporting communication with parents and staff.
- Improving administration and monitoring.

Risks

REACH recognises that risks include:

- Exposure to harmful or inappropriate content.
- Grooming, exploitation, and online radicalisation.
- Sexting, sharing of illicit images, and cyberbullying.
- Gaming and gambling risks (e.g. loot boxes, chat rooms).
- Livestreaming, influencer pressure, and unsafe online challenges.
- AI-generated content and deepfakes used for manipulation or bullying.

Management

- Internet access is filtered and monitored in line with DfE standards.
- Staff and students are trained in recognising unsafe or misleading content.
- Use of personal devices by staff and students is controlled and monitored.
- Data is protected under GDPR and the REACH Data Protection Policy.

Specific Guidance

Email

- Staff use provision-issued email accounts only.
- Communication with students and parents must remain professional.
- Offensive, threatening, or unsuitable emails must be reported.

Images & Media

- Parental consent is required for external/public use of student images.
- Images are stored securely and never published with full names.
- Parents/carers are not permitted to take images on site.

Social Media

- Staff must maintain professional boundaries and never use personal accounts to contact students.
- Students are taught risks of social networking, sexting, and oversharing.
- Misuse is managed via the Behaviour and Safeguarding policies.

Mobile Devices

- Student phones must be handed in or stored securely during provision hours.
- Staff must not use personal devices for student photos, videos, or communication.
- Emergencies are managed via the provision office.

Responding to Incidents

Illegal Incidents

- Child sexual abuse material, grooming, or other criminal activity will be referred immediately to the police and safeguarding authorities.

Inappropriate Incidents

Handled via Behaviour and Disciplinary procedures. Sanctions may include:

- Warning, loss of ICT access, behaviour contract.
- Referral to DSL or external agencies.
- Suspension or permanent exclusion for repeated/serious misuse.

Staff breaches may lead to:

- Formal disciplinary action.
- Referral to HR, Local Authority, or the police.

All incidents are logged and reviewed to inform future practice.

Education & Training

- E-safety is taught through ICT, PSHE, and across the curriculum.
- Staff receive annual training, with induction training for all new starters.
- Parents/carers receive information via workshops, newsletters, and the REACH website.

Monitoring & Review

- Filtering and monitoring systems are reviewed termly.
- Policy reviewed annually by DSL and trustees, or sooner if guidance changes.
- Incidents and evaluations inform continuous improvement.

Related Policies

- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- GDPR & Data Protection Policy
- Drugs & Substance Misuse Policy