POLICY

E-SAFETY

Approval Date	**September 2026**
Review Date	**September 2027**
Owner	

Policy Type		
		Trust Policy to be adopted in full
	■	Trust Policy adapted by the School
		School Policy

Approval Body		
	■	Executive
		Trust Board
		Local Advisory Body (LAB)

020 8290 8505
www.orionedu.org.uk
enquiries@orionedu.org.uk

Orion Education
Mansion House, Coopers School
Hawkwood Lane, Chislehurst,
Kent BR7 5PS

Orion Education

Our Four Critical Questions

Why do we exist?

To improve outcomes, transform lives and enable social mobility.

How do we behave?

Trust • Kindness • Endeavour

What do we do?

We create a strong network of schools which transform the lives of students by enabling them to achieve high educational and personal goals, regardless of their background.

How do we succeed?

Through a clear backbone, strong culture, academic rigour and smart systems.

1. Introduction & Scope

This policy outlines the collective commitment of our primary and secondary phases to ensure a safe digital environment. It covers all network infrastructure, devices, and personal devices used on school premises. It is aligned fully with the latest Keeping Children Safe in Education (KCSIE) statutory directives.

2. The 'Four Cs' Risk Framework

We continuously assess and manage online activities through the standard UK safeguarding filters:

- Content: Mitigating exposure to age-inappropriate, radical, or harmful material.
- Contact: Stopping peer-on-peer grooming, stranger manipulation, or unsafe dialogue.
- Conduct: Tackling cyberbullying, digital exclusion, and text/image-based harassment.
- Commerce: Defending users against identity theft, gambling prompts, and financial scams

3. Phase-Specific Differentiations

To address the varying development levels across pupils, our school implements a dual-layered management system:

Policy Domain	Primary Phase (KS1/KS2)	Secondary Phase (KS3/KS4/KS5)
Filtering & Filtering Levels	High restriction; strict whitelisting; search queries restricted to verified platforms.	Balanced monitoring; age-appropriate blacklisting; allowed access to curated social research data.
Personal Devices	Strictly forbidden on premises. Left in lockers or with reception staff.	Permitted on site under a 'gate-to-gate' policy. Disabled during formal lessons.
Digital Education Focus	Basic digital citizenship, reporting strange pop-ups, and identifying trusted adults.	Fact-checking AI systems, media manipulation, digital footprints, and consent boundaries.

4. Acceptable Use Policy (AUP) Fundamentals

All stakeholders (pupils, staff, and external guests) must review and sign the Acceptable Use Agreements prior to receiving network authentication credentials. Staff must exclusively route communications through administrative channels and avoid direct linkages with students on private social media.

5. AI and Generative Technology Guidance

While text and visual AI tools are welcomed inside planned learning modules, student submissions must clearly mark generated content.

6. Reporting Pathways and Escalation

Any observed online harm, bypass of system filtering, or suspicious peer activity must immediately be forwarded to the designated safeguarding lead:

- Primary DSL: Samantha Anderson
- Secondary DSL: Cheryl Raithby