



ORANGE TREE SCHOOL

ONLINE SAFETY POLICY

2026-2027

Main Site and Ridgeway Hospital Provision

Independent School Standards: Part 1, paragraph 2; Part 2, paragraph 5; Part 3, paragraphs 7 and 11; Part 8, paragraph 34



DOCUMENT DETAILS	
Applies To:	• All Staff • External suppliers or visitors • Regulatory / Legal bodies • Other (e.g. Parents) • Hospital Staff
Policy Author:	Zoe Ramshaw
Approval Body:	Advisory Board – Peter Curtis
Frequency of review:	Annually
Last review date:	August 2025
Last Update:	01/08/2026
Next Review Date:	01/08/2027

Policy Summary

Purpose

Orange Tree School is committed to creating a safe, supportive and responsible digital environment in which pupils can benefit from technology while being protected from online harm. This policy explains how the school promotes online safety through safeguarding, education, filtering and monitoring, secure use of devices, professional practice and partnership with families.

The policy recognises that technology is used across the curriculum and is particularly important for pupils who use laptops as their normal way of working, as assistive technology or as part of examination access arrangements.

Core principles

- Online safety is an integral part of safeguarding and is everyone's responsibility.
- Pupils should benefit from digital technology without being exposed to avoidable risk.
- Online safety education must be personalised, developmentally appropriate and responsive to pupils' SEND and communication profiles.
- School-managed devices should be appropriately filtered, monitored and secured.
- Personally owned laptops and tablets are not normally permitted because the school cannot guarantee effective filtering, monitoring or technical security.
- Concerns arising online are treated with the same seriousness as concerns arising offline.
- The school promotes informed, responsible and ethical use of digital technology, including artificial intelligence.

Key expectations

- All staff understand their safeguarding responsibilities in relation to online activity.
- Pupils receive regular online safety education through the curriculum and in response to emerging needs.
- Filtering and monitoring arrangements, including Securus, are reviewed and acted upon appropriately.
- Pupils use school-managed devices and accounts in accordance with acceptable-use expectations.
- Staff report online safety concerns promptly to the Designated Safeguarding Lead (DSL).
- Parents and carers are supported to understand the school's approach and to promote safe technology use at home.

Content

S

Policy Summary.....	3
1. Introduction.....	5
2. Aims.....	5
3. Legal and Regulatory Framework.....	5
4. Understanding Online Risk.....	6
5. Digital Learning at Orange Tree School.....	6
6. School-Managed Devices and Accounts.....	7
7. Personally Owned Laptops and Tablets.....	7
8. Filtering and Monitoring.....	8
9. Online Safety Education.....	8
10. Supporting Pupils with SEND and Additional Vulnerabilities.....	9
11. Artificial Intelligence.....	9
12. Staff Professional Expectations.....	10
13. Images, Video, Audio and Online Publication.....	10
14. Cyberbullying, Harmful Content and Online Incidents.....	10
15. Reporting and Responding to Concerns.....	11
16. Partnership with Parents and Carers.....	11
17. Ridgeway Hospital Provision.....	12
18. Roles and Responsibilities.....	12
19. Training, Monitoring and Review.....	13
20. Related Policies and Documents.....	14

1. Introduction

Digital technology plays an important role in education, communication and everyday life. At Orange Tree School, pupils may use laptops and other digital tools to access learning, communicate, develop independence, complete assessments and take public examinations.

Although computing is taught formally at Key Stage 3, online safety applies to pupils of every age because digital technology is used across the curriculum and beyond school. Online safety is therefore not confined to computing lessons; it is embedded within safeguarding, relationships education, personal development and day-to-day teaching.

As a specialist independent school for pupils with Education, Health and Care Plans, Orange Tree recognises that some pupils may require explicit and repeated teaching about online relationships, privacy, consent, harmful content, misinformation, manipulation, exploitation and safe communication. Support will reflect each pupil's developmental stage, communication profile, emotional wellbeing, SEND and individual risk assessment.

This policy should be read alongside the School's Safeguarding and Child Protection Policy, Mobile Phone and Personal Devices Policy, Cyber Security Policy, Data Protection Policy, Staff Code of Conduct and Acceptable Use Agreements.

2. Aims

The aims of this policy are to:

- protect pupils from online harm and ensure concerns are identified and acted upon promptly;
- enable pupils to use technology safely, responsibly and confidently;
- provide clear expectations for staff, pupils, parents, contractors and visitors;
- ensure appropriate filtering and monitoring systems are in place and reviewed;
- support equitable access to technology for learning, SEND and examination arrangements;
- promote digital literacy, critical thinking, respectful communication and informed decision-making;
- ensure the safe and lawful use of personal data, images, video, online platforms and artificial intelligence; and
- maintain effective governance, accountability and continuous improvement.

3. Legal and Regulatory Framework

This policy has been developed with regard to:

- The Education (Independent School Standards) Regulations 2014;
- Keeping Children Safe in Education (current edition);
- Working Together to Safeguard Children (current edition);
- The Equality Act 2010;
- The Children Act 1989 and Children Act 2004;
- The Data Protection Act 2018, UK GDPR and the Data (Use and Access) Act 2025;

- The Computer Misuse Act 1990;
- The Voyeurism (Offences) Act 2019 and Online Safety Act 2023 where relevant;
- Department for Education filtering and monitoring standards for schools and colleges;
- Department for Education cyber security and digital technology standards;
- Department for Education statutory guidance on mobile phones in schools; and
- Department for Education guidance on the safe use of generative artificial intelligence in education.

The school will keep its arrangements under review as legislation, statutory guidance, digital technology and patterns of online harm develop.

4. Understanding Online Risk

Online risks may occur through school systems, personal devices, social media, messaging, gaming, live streaming, online communities, artificial intelligence tools or other digital services. The School uses the four broad areas of risk commonly described in safeguarding guidance:

Content

Exposure to illegal, harmful, misleading or age-inappropriate material, including pornography, self-harm or suicide content, extremist material, violence, eating-disorder content, hate content, misinformation and AI-generated material.

Contact

Harmful interaction with others online, including grooming, coercion, exploitation, harassment, sexual solicitation, impersonation and contact with unknown adults or peers.

Conduct

The pupil's own behaviour online, including cyberbullying, sharing personal information, recording others, sexting or sharing nude or semi-nude images, abusive communication, unsafe challenges and breaches of privacy or copyright.

Commerce

Risks associated with advertising, scams, gambling-like features, in-app purchases, phishing, financial exploitation and pressure to buy, trade or transfer money or digital items.

The school also recognises the risks of compulsive or excessive use, disrupted sleep, online dependency, social comparison, harmful online relationships and the impact of online experiences on anxiety, regulation, attendance and learning.

5. Digital Learning at Orange Tree School

Technology is used across Orange Tree School to support curriculum access, communication, assessment and independence. This may include:

- laptops as a normal way of working;
- assistive technology and accessibility tools;

- word processing, research and presentation software;
- online learning platforms and curriculum resources;
- communication and visual-support tools;
- assessment and examination access arrangements; and
- personalised learning during hospital admission, transition or reintegration.

Digital access will be purposeful, supervised according to need and balanced with direct teaching, discussion, practical learning, reading, writing, movement and social interaction. Technology should enhance learning rather than replace appropriate relationships or teaching.

6. School-Managed Devices and Accounts

Where a pupil requires a laptop or other device for learning, SEND, communication or examinations, the school will normally provide or approve a school-managed device. School-managed devices are configured to support appropriate filtering, monitoring, security, software management and technical support.

Pupils must:

- use only their authorised account and keep passwords private;
- use devices for agreed educational purposes;
- follow staff instructions and acceptable-use expectations;
- not attempt to bypass filtering, monitoring, security settings or restrictions;
- not download or install unapproved software, browser extensions or virtual private networks;
- not access, alter or delete another person's files or account;
- report harmful content, suspicious messages, security alerts or accidental access promptly; and
- take reasonable care of devices and return them when required.

School-managed devices may be monitored when used on or away from the school site, in accordance with the school's safeguarding, data-protection and acceptable-use arrangements.

7. Personally Owned Laptops and Tablets

As a general rule, pupils are not permitted to bring personally owned laptops or tablets into school for educational use. This is because the school cannot guarantee that personal devices are appropriately configured, filtered, monitored, updated or secured, and cannot reliably protect pupils, other users, school data or the network from associated risks.

The school will provide a suitable managed device where a laptop is required as a pupil's normal way of working or as part of an agreed access arrangement.

An exception may be authorised by the Headteacher only where there is a clear educational, medical or accessibility reason and a written risk assessment confirms that appropriate safeguarding, filtering, monitoring, security, data-protection and technical arrangements can be maintained. Permission may be withdrawn if the arrangements are no longer safe or effective.

Mobile phones, smart watches and other personal communication devices are governed by the School's Mobile Phone and Personal Devices Policy.

8. Filtering and Monitoring

Orange Tree School maintains filtering and monitoring arrangements designed to reduce access to harmful and inappropriate content and to identify activity that may indicate a safeguarding concern.

The school currently uses Securus as its filtering and monitoring system, supported by its external IT provider and internal safeguarding processes.

Filtering and monitoring are safeguards, but they cannot replace staff vigilance, supervision, education and professional curiosity. Staff remain responsible for observing how pupils use technology and responding to changes in presentation, language or behaviour.

The school will:

- assign clear responsibility for filtering and monitoring to the Headteacher, DSL, relevant operational lead and IT provider;
- review filtering and monitoring arrangements at least annually and following significant incidents or technological change;
- ensure filtering does not unreasonably restrict appropriate teaching and learning;
- ensure monitoring alerts and reports are reviewed by appropriately trained staff within agreed timescales;
- maintain an escalation and response process for concerns identified through monitoring;
- consider the needs of pupils using school-managed devices away from the school network;
- ensure staff understand the limitations of the systems and how to report concerns; and
- record decisions, actions and lessons learned where significant concerns arise.

Attempts to disable or circumvent filtering or monitoring will be treated seriously and may constitute a safeguarding, behaviour or cyber-security concern.

9. Online Safety Education

Online safety will be taught through computing, PSHE, Relationships and Sex Education, personal development, assemblies, tutor work and responsive teaching. Teaching will be revisited regularly and adapted to emerging risks and the needs of individual pupils.

Pupils will be supported to understand, where developmentally appropriate:

- how to protect personal information, passwords, images and location data;
- how online content is selected, promoted, manipulated or generated;
- how to recognise misinformation, scams, grooming, coercion and harmful contact;
- privacy, consent, respectful communication and digital footprints;
- cyberbullying and how to seek help;
- safe and lawful use of images, video, live streaming and online communication;
- risks associated with gaming, social media, online communities and in-app purchases;
- how online activity can affect sleep, mood, anxiety, regulation and relationships;
- how to report concerns, block users, preserve evidence and access trusted support; and
- appropriate and ethical use of artificial intelligence.

- Learning will be adapted to reflect pupils' age, developmental stage, communication needs, EHCP outcomes and individual risk assessments.

The school will not assume that a pupil who appears technically confident understands social, emotional, legal or safeguarding risks.

10. Supporting Pupils with SEND and Additional Vulnerabilities

All pupils at Orange Tree School have SEND. Online safety support must therefore be personalised and integrated with each pupil's EHCP provision, communication profile, risk assessment and therapeutic support where appropriate.

Some pupils may:

- interpret online communication literally or find it difficult to recognise sarcasm, deception or manipulation;
- be more trusting of people met online or seek belonging through online communities;
- find it difficult to understand privacy, consent, boundaries or the permanence of online content;
- become intensely focused on particular games, platforms, topics or relationships;
- use online spaces to manage anxiety or social isolation and become distressed when access changes;
- be vulnerable to coercion, exploitation, radicalisation, financial scams or harmful influence;
- experience increased dysregulation, self-harm thoughts, eating difficulties or anxiety following online exposure; or
- require alternative communication methods to disclose online harm.

Support may include explicit teaching, visual resources, social narratives, modelling, repetition, supervised practice, individual boundaries, parental partnership, therapeutic input and individual online-safety or risk-management plans. Restrictions should be proportionate, regularly reviewed and combined with teaching that develops increasing independence.

11. Artificial Intelligence

Artificial intelligence can support planning, accessibility, creativity and learning, but may also produce inaccurate, biased, manipulative or inappropriate content. It can create risks relating to privacy, safeguarding, intellectual property, academic integrity and over-reliance.

Staff and pupils must not enter personal, confidential, safeguarding, medical, staff, pupil or commercially sensitive information into an AI tool unless that tool has been expressly approved by the school for that purpose and appropriate data-protection arrangements are in place.

Where AI is used:

- its use must have a clear educational or professional purpose;
- users must critically check accuracy, bias, suitability and source reliability;

- AI output must not replace professional judgement, safeguarding decision-making or direct knowledge of a pupil;
- pupils must be taught when and how to acknowledge AI assistance;
- AI must not be used to impersonate, harass, sexualise, exploit or create harmful images or content about another person;
- age restrictions and product-safety considerations must be followed; and
- any concerning AI-generated content or use must be reported promptly.

The school may issue separate operational guidance as AI technology and official guidance continue to develop.

12. Staff Professional Expectations

Staff must model safe, respectful and professional digital behaviour. Staff are expected to:

- use school-approved accounts, systems and communication channels for school business;
- maintain professional boundaries in all online contact with pupils and families;
- not communicate privately with pupils through personal social-media accounts, personal messaging apps or personal email;
- not use personal devices to photograph, film or record pupils, meetings or confidential information unless specifically authorised under an agreed school procedure;
- protect passwords, use multi-factor authentication where required and lock devices when unattended;
- follow data-protection, cyber-security, acceptable-use and records-management requirements;
- check online resources before use and supervise access according to pupil need;
- report harmful content, monitoring alerts, suspected breaches, online allegations or concerning pupil activity promptly;
- not investigate safeguarding concerns independently beyond what is necessary to preserve immediate safety and evidence; and
- complete required online-safety, filtering and monitoring training.

Any allegation about a member of staff's online conduct must be managed in accordance with the Safeguarding and Child Protection Policy, Staff Code of Conduct and procedures for allegations and low-level concerns.

13. Images, Video, Audio and Online Publication

Images, video and audio can create lasting safeguarding and privacy risks. The school will obtain and record appropriate permissions and will use content only for agreed purposes.

Pupils, parents, visitors and staff must not photograph, film or record pupils, staff, meetings, lessons or activities on site without explicit authorisation. School-authorised recording must use approved equipment and storage arrangements.

Before publishing content online, staff must consider consent, safeguarding, identifying information, location, uniform, metadata, dignity and whether publication remains in the pupil's best interests. Concerns about the sharing or misuse of images must be reported immediately.

14. Cyberbullying, Harmful Content and Online Incidents

Online behaviour that affects a pupil's safety, wellbeing, relationships or education may be addressed by the school even where it occurs outside school or on a personal device.

Responses will be proportionate and may include:

- immediate safeguarding action and DSL involvement;
- support for the pupil affected and any other pupils involved;
- preserving relevant evidence without unnecessarily viewing or sharing harmful content;
- contact with parents or carers;
- education, reflection and restorative work where appropriate;
- review of individual risk assessments and support plans;
- referral to the police, Local Authority, social care, Prevent partners or other agencies where required;
- reporting content to a platform or service; and
- action under the Relationship and Regulation Policy, Mobile Phone and Personal Devices Policy or Staff Code of Conduct.

The school will avoid automatically treating a pupil who has experienced online harm as responsible for that harm. Responses will consider vulnerability, coercion, developmental understanding, SEND and the wider context.

15. Reporting and Responding to Concerns

Any online safety concern involving a pupil must be reported promptly to the DSL or a Deputy DSL through the School's safeguarding reporting arrangements. Immediate danger must be addressed without delay and emergency services contacted where necessary.

Staff should record:

- what was observed, disclosed or reported;
- the pupil's own words where possible;
- the device, account, platform or service involved;
- any immediate action taken;
- whether evidence has been preserved; and
- who has been informed.

Staff must not forward, copy or store illegal or sexual images of children. Where such material is suspected, staff must follow safeguarding guidance and seek immediate direction from the DSL.

Cyber-security or data-protection incidents must also be reported in accordance with the Cyber Security Policy and Data Protection Policy.

16. Partnership with Parents and Carers

The school recognises that pupils' online lives cross the boundary between school and home. Effective online safety therefore requires respectful partnership with parents and carers.

The school will:

- communicate its expectations regarding mobile phones, personal devices and school-managed technology;
- provide advice or signposting about emerging online risks and parental controls where appropriate;
- work collaboratively where online activity affects attendance, wellbeing, relationships or learning;
- explain why personally owned laptops and tablets are not normally permitted;
- involve parents in individual risk-management plans where appropriate; and
- ensure urgent safeguarding concerns are shared in accordance with safeguarding procedures.

Parents and carers are expected to support the School's policies, communicate concerns promptly and avoid contacting pupils during the school day through personal devices except through agreed school arrangements.

17. Ridgeway Hospital Provision

At Ridgeway, online safety arrangements will take account of the shared hospital environment, clinical needs, individual education plans, length of admission, home-school systems and any restrictions or risk-management arrangements agreed with the clinical team.

Ridgeway staff will:

- clarify which organisation provides, filters, monitors and manages each device or network;
- ensure education staff understand relevant hospital procedures and escalation routes;
- liaise with home schools regarding managed devices, accounts and curriculum access;
- consider the impact of medical, psychological and emotional presentation on online risk;
- include online safety in transition and reintegration planning where relevant; and
- report concerns through both School and hospital safeguarding routes where required.

18. Roles and Responsibilities

Advisory Board

- provide strategic oversight and assurance that online safety arrangements meet safeguarding and Independent School Standards requirements;
- receive assurance about filtering and monitoring, significant incidents, training and emerging risks;

- ensure sufficient resources and expertise are available.

Headteacher

- ensure this policy is implemented across both sites;
- allocate clear operational responsibility for digital safeguarding, filtering and monitoring;
- ensure personal-device exceptions are authorised only following appropriate assessment;
- ensure significant concerns are reported to the Advisory Board.

Designated Safeguarding Leads

- take lead responsibility for online safety within safeguarding arrangements;
- understand filtering and monitoring systems, reports and escalation processes;
- ensure concerns are assessed, recorded, escalated and reviewed;
- ensure staff receive appropriate training and updates.

Teaching and Learning Lead

- ensure online safety is embedded across curriculum planning and teaching;
- support staff to provide developmentally appropriate and SEND-responsive education;
- monitor the quality and consistency of classroom practice.

IT and Operational Leads / External IT Provider

- maintain agreed technical controls, accounts, updates and device management;
- support filtering, monitoring, cyber-security, backup and incident response;
- provide timely information to the Headteacher and DSL;
- avoid making safeguarding judgements that belong to school leaders.

All Staff

- follow this policy and associated acceptable-use expectations;
- supervise and educate pupils appropriately;
- remain vigilant to online harm and report concerns promptly;
- protect data, accounts, devices and professional boundaries.

Pupils

- use technology safely, respectfully and for agreed purposes;
- follow staff instructions and acceptable-use expectations;
- report concerns and seek help from a trusted adult;
- respect other people's privacy, dignity, work and property.

Parents and Carers

- support the school's online safety and device expectations;
- share relevant concerns and changes in risk;
- work with the school to support safe and balanced use of technology.

19. Training, Monitoring and Review

All staff will receive online safety training at induction and regular updates thereafter. Staff with designated responsibilities for safeguarding, filtering, monitoring, data protection or technical systems will receive role-appropriate training.

The Headteacher and DSL will monitor the effectiveness of this policy through:

- filtering and monitoring reviews and incident reports;
- safeguarding records and trend analysis;
- curriculum review, learning walks and pupil voice;
- staff training records and confidence checks;
- review of device, network and account arrangements;
- parent feedback and emerging concerns;
- review of individual risk assessments and support plans; and
- termly assurance to the Advisory Board.

This policy will be reviewed annually, or sooner following significant incidents, changes to legislation or guidance, introduction of new technology, or changes to School arrangements.

20. Related Policies and Documents

- Safeguarding and Child Protection Policy
- Mobile Phone and Personal Devices Policy
- Cyber Security Policy
- Data Protection Policy
- Staff Code of Conduct
- Relationship and Regulation Policy
- Anti-Bullying Policy
- Preventing Radicalisation and Extremism Policy
- Remote Learning Policy
- CCTV Policy
- Risk Assessment Policy
- Teaching and Learning Policy
- Acceptable Use Agreements
- Educational Visits Policy
- Complaints Policy