Vita et Pax
PREPARATORY SCHOOL

Vita et Pax Preparatory School
Established 1936

Online Safety Policy

Policy Originator	Darren May & Kate Newton
Chair of Governors	Pushkar Acharya
Date Approved	1 March 2026
Status	Statutory
Review Period	Annually (next: March 2027)

This policy applies to all members of the school community — staff, pupils, governors, volunteers, visitors and contractors — who have access to school systems, devices and networks. It should be read alongside the school's Safeguarding & Child Protection Policy, IT Acceptable Use Policy, Behaviour & Discipline Policy, and Staff Code of Conduct.

1. Purpose and Scope

The purpose of this policy is to:

- Safeguard and protect all members of the school community online.
- Set clear expectations for online behaviour and use of technology.
- Establish a robust framework for filtering and monitoring online activity, as required by KCSIE 2025.
- Educate pupils, staff and parents about online risks and responsible digital citizenship.
- Ensure the school meets its statutory obligations under the Independent School Standards Regulations (ISSRs) 2014 and KCSIE 2025.

2. Legislation and Guidance

This policy is informed by:

- Keeping Children Safe in Education (September 2025) — Part 2 (management of safeguarding) and paragraphs on filtering and monitoring.
- Working Together to Safeguard Children (2023).
- Relationships Education, RSE and Health Education (2024).
- Digital and Technology Standards for Schools and Colleges (DfE, 2023).

- Teaching Online Safety in Schools (DfE, 2023).
- Searching, Screening and Confiscation (DfE, 2022).
- The Data Protection Act 2018 and UK GDPR.
- The Voyeurism (Offences) Act 2019 (upskirting).
- The Online Safety Act 2023.
- The Sexual Offences Act 2003.
- The Education Act 2011 (staff powers to search and delete).

3. Roles and Responsibilities

The Governing Body will:

- Ensure the school has appropriate filtering and monitoring systems in place.
- Review the effectiveness of online safety measures at least annually.
- Ensure staff receive appropriate online safety training.
- Receive termly reports on online safety incidents and filtering effectiveness.

The Head Teacher (Darren May) will:

- Take overall responsibility for online safety as part of the safeguarding role.
- Ensure this policy is implemented and followed by all staff.
- Ensure online safety is embedded across the curriculum.
- Report online safety matters to the governing body.

The DSL / Deputy DSL (Darren May / Kate Newton) will:

- Take lead responsibility for online safeguarding concerns.
- Ensure filtering and monitoring systems are reviewed at least annually and that the school meets the DfE filtering and monitoring standards.
- Act on online safety alerts generated by NeuralShield and other monitoring tools.
- Liaise with the MASH and police where online activity raises safeguarding concerns.
- Log all online safety incidents and maintain records for audit.

All Staff will:

- Read and follow this policy and the IT Acceptable Use Policy.
- Maintain an awareness of current online safety issues and risks.
- Report any online safety concerns to the DSL immediately.
- Model safe and responsible use of technology.
- Integrate online safety into teaching and the wider curriculum.
- Not use personal devices to photograph or record pupils (see EYFS section).

Parents and Carers are expected to:

- Read the school's online safety guidance and support its implementation at home.
- Report any online safety concerns to the school promptly.
- Supervise children's online activity at home in an age-appropriate manner.
- Be aware of the age restrictions on social media and gaming platforms.

4. Filtering and Monitoring

KCSIE 2025 requires schools to ensure appropriate filtering and monitoring systems are in place. The school operates NeuralShield, an AI-powered network safeguarding system that provides:

- DNS-level content filtering — blocking access to illegal content, harmful material, and age-inappropriate websites across all school devices and networks.
- Real-time network monitoring — identifying unusual patterns of online activity that may indicate safeguarding concerns.
- Automated alerts — notifying the DSL and designated staff of filtering breaches and concerning online behaviour.
- Category-based blocking — content categories including extremism, pornography, violence, self-harm, drugs, and gambling are blocked by default.

NeuralShield meets the DfE's Filtering and Monitoring Standards (2023). The system is:

- Effective across all school-managed devices and networks (including Wi-Fi).
- Age-appropriate — different filtering profiles may apply to different year groups.
- Reviewed at least annually by the DSL and IT Lead for effectiveness.
- Not reliant on a single system — layered with additional controls on managed devices.
- Reported on termly to the governing body, including blocked content statistics and any safeguarding alerts generated.

Staff should be aware that no filtering system is 100% effective. Education and vigilance remain essential. If a pupil encounters harmful material despite filtering, the incident should be reported to the DSL and the IT Lead immediately.

Filtering can be adjusted for legitimate educational purposes by the IT Lead, with approval from the DSL. Any 'override' requests are logged and reviewed.

5. Online Risks

Online safety risks can be categorised into four areas:

- Content — being exposed to illegal, inappropriate or harmful content (e.g. pornography, violence, self-harm, fake news, racist or hateful material).
- Contact — being subjected to harmful online interaction with other users (e.g. grooming, commercial exploitation, bullying, identity theft).
- Conduct — children's own online behaviour that increases the likelihood of, or causes, harm (e.g. sharing nude images, online bullying, plagiarism, hacking).
- Commerce — risks such as online gambling, inappropriate advertising, phishing, financial scams and in-app purchases.

Specific risks include:

- Child sexual exploitation and abuse (CSEA) — children being groomed or coerced online for sexual purposes.
- Cyberbullying — bullying via digital devices, platforms or messaging.
- Online grooming — adults building relationships with children online for the purpose of sexual exploitation, criminal exploitation or radicalisation.

• Sexting / youth-produced sexual imagery — the sharing of nude or semi-nude images by children. This can constitute a criminal offence.

• Radicalisation and extremism — exposure to extremist ideologies and recruitment online (see Prevent Duty section).

• Harmful online challenges and hoaxes — dangerous challenges promoted on social media platforms.

• Excessive screen time — impacting mental health, sleep and wellbeing.

• Generative AI — risks associated with AI chatbots, deepfakes, and AI-generated content including non-consensual imagery.

6. Responding to Online Safety Incidents

6.1 General Procedure

When an online safety incident occurs:

• Report to the DSL immediately.

• Do not forward, share or save indecent images — this is a criminal offence.

• Secure and preserve evidence (do not delete).

• The DSL will assess whether the incident constitutes a safeguarding concern and whether referral to the MASH, police or other agencies is required.

• Parents of affected children will be informed unless doing so would increase risk.

• All incidents are logged and recorded.

6.2 Sexting / Youth-Produced Sexual Imagery

The school follows the guidance in KCSIE 2025 and the UK Council for Internet Safety (UKCIS) framework. Key principles:

• The incident is referred to the DSL immediately.

• The DSL assesses the situation — is the child at risk? Is it consensual? Are there aggravating factors (e.g. coercion, adult involvement)?

• Images must never be viewed, copied, printed or shared by staff unless specifically directed by the police or children's social care.

• Devices may be confiscated and secured for the police if a criminal offence may have been committed.

• The school may search devices in accordance with the Education Act 2011.

6.3 Online Bullying (Cyberbullying)

Cyberbullying is dealt with under the school's Behaviour & Discipline Policy and Anti-Bullying Policy. Staff should:

• Take all reports seriously.

• Advise the pupil not to retaliate or respond.

• Help the pupil to save/screenshot evidence.

• Report to the DSL and follow the school's behaviour procedures.

• Contact parents of both victim and perpetrator.

• Consider whether the bullying should be reported to the police or social care.

7. Use of Personal Devices and Mobile Phones

- Staff: Personal mobile phones must not be used in the presence of children and must be stored securely during teaching time. Personal devices must never be used to photograph or record pupils.
- EYFS: Mobile phones and personal cameras are strictly prohibited in all EYFS areas at all times.
- Pupils: Pupils are not permitted to bring mobile phones or smart devices into school. Any devices brought in must be handed to the school office.
- Visitors: Visitors are informed of the school's mobile phone policy on arrival and are expected to comply.
- School cameras and devices are used for any photography of pupils, and images are stored securely on school systems only.

8. Social Media

- Staff must not communicate with pupils or parents via personal social media accounts.
- Staff should be aware that their online conduct outside school could impact their professional reputation and position.
- Staff must not post images or information about school, pupils or colleagues on personal social media without explicit permission.
- Official school social media accounts are managed by designated staff only.
- Pupils are educated about the risks of social media, including age restrictions (most platforms require users to be 13+).

9. Online Safety in the Curriculum

Online safety is embedded across the curriculum, not taught in isolation. The school delivers age-appropriate online safety education through:

- Computing lessons — digital literacy, responsible use of technology, understanding algorithms and AI.
- PSHE / RSE — healthy relationships online, consent, body image, self-esteem and resilience.
- Assemblies — thematic online safety messages and awareness campaigns (e.g. Safer Internet Day, Anti-Bullying Week).
- Cross-curricular — critical evaluation of online sources in all subjects.

Teaching covers the four risk categories (content, contact, conduct, commerce) and includes topics such as: password security, privacy settings, recognising fake profiles, understanding age ratings, reporting mechanisms, and the permanence of online actions.

10. Data Protection and Online Security

- The school processes personal data in accordance with the Data Protection Act 2018 and UK GDPR (see Data Protection Policy).
- Strong passwords are required for all school accounts and systems.

- Staff must not share login credentials.
- Data breaches involving online systems must be reported to the Data Protection Co-ordinator (Maria Castro) and the Head Teacher immediately.
- Cloud-based systems used by the school are reviewed for data security and GDPR compliance before adoption.
- Parent and pupil consent for photography and online image use is obtained annually and recorded centrally.

11. Prevent Duty and Online Radicalisation

The Prevent Duty (Counter-Terrorism and Security Act 2015) requires the school to have due regard to preventing people from being drawn into terrorism. The internet is a significant tool for radicalisation.

- NeuralShield blocks access to known extremist and radicalisation content.
- Staff are trained to recognise signs of online radicalisation.
- Any concerns about a pupil being exposed to extremist material online are reported to the DSL, who will refer to the Channel programme or police Prevent team as appropriate.
- The school teaches critical thinking skills to build resilience against extremist narratives.

12. Remote and Online Learning

When the school provides remote learning (including live lessons), the following safeguards apply:

- Live lessons are conducted via school-approved platforms only.
- A member of staff hosts all live sessions; lessons are not recorded unless necessary and with prior notification.
- Pupils must have their camera on during live lessons for safeguarding purposes.
- A parent or carer should be aware that a live lesson is taking place.
- Staff must deliver live lessons from a professional setting (not bedrooms).
- The school's code of conduct and behaviour policy apply during remote learning.
- IT Acceptable Use Policy applies to all remote activity on school-issued devices.

13. Training

- All staff receive online safety training as part of safeguarding induction.
- The DSL and Deputy DSL receive enhanced online safety training as part of their Level 3 child protection training.
- All staff receive regular updates on emerging online risks.
- Online safety training is refreshed at least annually.
- Governors receive online safety awareness training.

14. Review and Monitoring

This policy is reviewed annually by the DSL and ratified by the governing body. The effectiveness of the policy is monitored through:

- Termly NeuralShield filtering and monitoring reports.
- Analysis of online safety incident logs.
- Staff and pupil surveys on online safety awareness.
- Annual review of the DfE filtering and monitoring standards checklist.
- Feedback from parents and the school community.

Approved by: Governing Body of Vita et Pax Preparatory School

Date: 1 March 2026