Vita et Pax
PREPARATORY SCHOOL

Vita et Pax Preparatory School
Established 1936

IT Acceptable Use Policy

Policy Originator	Head Teacher
Approved by	Governing Body
Date Approved	1 March 2026
Status	Statutory
Review Period	Annually (next: March 2027)

1. Introduction and Scope

This policy sets out the acceptable use of information technology at Vita et Pax Preparatory School. It applies to all members of the school community — including staff, governors, pupils, parents, visitors, volunteers and contractors — who access school IT systems, networks or devices in any capacity.

This policy is informed by:

- Keeping Children Safe in Education (KCSIE) 2025 — particularly the requirements for filtering and monitoring.
- The Online Safety Act 2023.
- The Data Protection Act 2018 and UK GDPR.
- The Computer Misuse Act 1990.
- The Copyright, Designs and Patents Act 1988.
- The Independent School Standards Regulations (ISSRs) 2014.
- DfE guidance: Filtering and Monitoring Standards for Schools and Colleges (2023).
- The Statutory Framework for the Early Years Foundation Stage (EYFS) 2024.
- The school's Child Protection & Safeguarding Policy.

Access to school IT systems is a privilege, not a right. Breaches of this policy may result in disciplinary action and/or restriction of access.

2. Network Filtering and Monitoring — NeuralShield

The school operates NeuralShield, an AI-powered network safeguarding system that provides comprehensive filtering and monitoring of all internet traffic across the school network. NeuralShield is a core component of the school's duty to safeguard children online, as required by KCSIE 2025.

2.1 Filtering

NeuralShield operates at the DNS and network level to block access to harmful and inappropriate content, including:

- Illegal content (child sexual abuse material, terrorist content).
- Content harmful to children (pornography, extreme violence, self-harm, pro-anorexia, drug use, weapons).
- Extremist and radicalisation material.
- Known phishing, malware and command-and-control domains.
- Gambling, proxy/VPN bypass services and anonymisation tools.

The filtering system uses AI-driven classification to identify and block harmful content in real time, supplemented by regularly updated blocklists. Filtering cannot be overridden by pupils and can only be adjusted by authorised IT staff.

2.2 Monitoring

NeuralShield continuously monitors network activity to detect safeguarding concerns, including:

- Attempts to access blocked content (logged and reviewed).
- Unusual or concerning search terms and browsing patterns.
- Potential indicators of grooming, exploitation, radicalisation or self-harm.
- Unauthorised device connections to the school network.
- Data exfiltration or suspicious network behaviour.

Monitoring alerts are reviewed by the IT Lead and escalated to the DSL (Darren May) where a safeguarding concern is identified. Monitoring data is stored securely and retained in accordance with the school's data retention policy. The system generates regular reports for the DSL and the proprietorial body.

2.3 Review and Oversight

The effectiveness of filtering and monitoring is reviewed termly by the DSL and IT Lead. The proprietorial body receives an annual report on filtering and monitoring effectiveness, as required by KCSIE 2025. The school ensures that filtering and monitoring systems are proportionate, do not unreasonably restrict access to legitimate educational resources, and are regularly tested.

3. Online Behaviour — All Users

All members of the school community must observe the following principles in their online activities:

- Online communications must be respectful, professional and appropriate. Do not create, access or share content that is illegal, offensive, discriminatory, extremist or that raises safeguarding concerns.
- Respect the privacy of others. Do not share photographs, videos, contact details or other information about members of the school community without appropriate permission.

• Copyright: Do not access or share material that infringes copyright. Do not claim the work of others as your own.

• Security: Do not use the internet to distribute malware, gain unauthorised access to systems, or carry out any illegal activity.

• Staff–pupil boundaries: Staff must not use personal email or social media accounts to contact pupils or parents. Pupils and parents must not attempt to contact staff via personal channels.

4. Using School IT Systems

• Access school systems only with your own username and password. Never share credentials with anyone.

• Do not attempt to circumvent content filters, NeuralShield protections or other security measures. Do not use VPNs, proxies or anonymisation tools to bypass school filtering.

• Do not install software on school devices without IT authorisation.

• Do not connect personal devices to the school network without prior approval.

• School IT systems are provided for educational and professional purposes. Limited personal use by staff is permitted provided it does not interfere with duties, compromise security or contravene this policy.

• Be aware that the school monitors all use of school IT systems, including internet browsing history, email content and network activity.

5. Password Security

• Passwords must be strong: at least 8 characters, mixing upper/lowercase, numbers and symbols. Avoid obvious passwords (names, birthdays, 'password123').

• Do not reuse school passwords on personal accounts.

• Do not share your password with anyone, including colleagues.

• Change your password immediately if you suspect it has been compromised.

• Do not write passwords down where they can be seen by others.

• Staff accounts with access to sensitive data use multi-factor authentication (MFA) where available.

6. Personal Devices and Remote Working

All official school business must be conducted on school systems. Use of personal devices for school purposes requires prior approval and must comply with the following safeguards:

• Personal devices used for school work must have a passcode/biometric lock and up-to-date antivirus software.

• School data must not be stored on personal devices without encryption.

• Removal of personal data or confidential information from school systems — by any means including email, printing, USB, cloud storage — must be approved in advance.

• When working remotely, staff must use secure connections and follow the same data protection standards as on site.

7. Mobile Phones and Cameras

• Staff: Personal mobile phones must not be used in teaching areas or in the presence of pupils. Phones should be stored securely in a bag, locker or the staffroom. Staff may use phones in the staffroom or during designated breaks.

• EYFS: Personal mobile phones and cameras are strictly prohibited in EYFS areas at all times. This applies to all adults, including staff, parents, visitors and volunteers.

• Pupils: Pupils may not bring mobile phones to school. If a phone is brought for safety reasons (e.g., walking home), it must be handed to the school office on arrival and collected at the end of the day.

• Photography: Only school-owned devices may be used to photograph or record pupils. Parental consent is obtained for all pupil photography. Images are stored securely on school systems and never on personal devices.

• Visitors: Visitors are informed of the mobile phone and camera policy on arrival and must not use personal devices to photograph or record in school.

8. Social Media

• Staff must not post content that could bring the school into disrepute or compromise their professional standing.

• Staff must not be 'friends' with or follow current pupils (or recent former pupils under 18) on personal social media.

• Staff should maintain the highest privacy settings on personal social media accounts.

• Any school-related social media is managed through official school accounts only.

• Negative or disparaging comments about the school, staff, pupils or parents on social media may be treated as a disciplinary matter.

9. Email

School email accounts are provided for professional and educational purposes. Staff must use school email (not personal email) for all school communications. Emails may be monitored. Staff should be professional and courteous in all email communications and should not use email to share confidential pupil data without appropriate safeguards (encryption or secure portal).

10. Artificial Intelligence (AI) Tools

The school recognises the growing use of AI tools (e.g., chatbots, image generators, writing assistants) in education and wider society. The school's position is:

• Staff may use approved AI tools to support planning, administration and professional development, provided no pupil personal data is entered into external AI systems.

• Pupils may only use AI tools under direct staff supervision and for approved educational purposes.

• AI-generated work must be clearly identified and not submitted as a pupil's own work.

- The school's AI systems (including NeuralShield) operate under strict data protection and safeguarding controls.
- Any new AI tools proposed for educational use must be risk-assessed by the IT Lead and DSL before deployment.

11. Data Protection and Breach Reporting

All use of school IT systems must comply with the Data Protection Act 2018 and UK GDPR. Personal data must be handled in accordance with the school's Privacy Notice and Data Protection Policy.

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes loss of devices, misdirected emails, hacking, and unsecure disposal. Examples:

- Loss of an unencrypted laptop, USB stick or physical file containing personal data.
- External hacking of school systems or malware infection.
- Misdirected email containing personal data.
- Failure to BCC recipients of a mass email.

All data breaches — suspected or confirmed — must be reported immediately to the Head Teacher and Data Protection Lead. The school will notify the ICO within 72 hours where required. Failure to report a breach is a disciplinary matter.

12. Online Safety Education for Pupils

The school teaches online safety as part of the computing and PSHE curriculum, covering:

- Keeping personal information private.
- Recognising and reporting cyberbullying.
- Understanding consent and respectful online communication.
- Critical evaluation of online content (fake news, misinformation).
- Understanding the risks of sharing images (including sexting/nudes).
- Age restrictions on social media and online services.
- Knowing how to report concerns to a trusted adult.

Online safety messages are reinforced through assemblies, Safer Internet Day activities and parent information sessions.

13. Retention of Digital Data

Emails sent or received on school systems are retained for up to 7 years. Email accounts are deleted within 1 year of the person leaving the school. Important records must be saved to the appropriate school system (not personal email folders). NeuralShield monitoring logs are retained in accordance with the data retention schedule and reviewed periodically.

14. Breaches of This Policy

Deliberate breaches of this policy will be dealt with as a disciplinary matter. For staff, this may include formal disciplinary proceedings. For pupils, the school's Behaviour & Discipline Policy applies. In addition, access to school IT systems may be restricted or withdrawn. Where a breach involves illegal activity, the matter will be referred to the police.

If you become aware of a breach of this policy, or you are concerned that a member of the school community is being harassed or harmed online, report it immediately to the Head Teacher or DSL.

15. Related Policies

- Child Protection & Safeguarding Policy
- Behaviour & Discipline Policy
- Anti-Bullying Policy
- Privacy Notice & Data Protection Policy
- Staff Code of Conduct
- RSE / PSHE Policy
- Educational Visits Policy
- Whistleblowing Policy

Approved by: Governing Body of Vita et Pax Preparatory School

Date: 1 March 2026