ABBEY COLLEGE IN MALVERN
abbeycollege.co.uk

Virtual Private Network (V.P.N.) Policy for Students

Related documents include:

- Keeping Children Safe in Education 2026 (Department for Education), in force from 1 September 2026.
- Department for Education, Meeting Digital and Technology Standards in Schools and Colleges: Filtering and Monitoring – Core Standard (updated 16 September 2026).
- Department for Education, Data Protection in Schools guidance, including the Data (Use and Access) Act 2025 compliance guidance (updated 14 October 2026).
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018, as amended.
- Data (Use and Access) Act 2025.
- Independent Schools Inspectorate, current inspection framework – Safeguarding, including expectations for effective and regularly reviewed online safety arrangements.

This policy should be read alongside the College's Safeguarding and Child Protection Policy, Online Safety Policy, Acceptable Use requirements, Behaviour and Discipline Policy and privacy information.

Legal Status:

There is no specific UK statute which prohibits students from using VPNs. The relevant legal and regulatory requirements concern safeguarding, online safety, filtering and monitoring, data protection, information security and the school's ability to protect pupils from harmful online content. This revised policy will therefore strengthen those areas without suggesting that VPN prohibition itself is a statutory requirement. The principal updates I have identified are:

KCSIE 2026: safeguarding responsibilities and protection from online harm.

DfE Filtering and Monitoring: Core Standard (updated 16 September 2026): expressly identifies VPNs, proxy services and other filtering circumvention technologies as risks that schools should address.

DfE digital standards: annual reviews, appropriate responsibilities for senior leadership, the DSL and IT support, and checks covering personal devices and college-managed devices.

Data protection: UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025, including appropriate transparency about monitoring and access to monitoring records.

ISI: the safeguarding inspection framework expects effective, regularly reviewed arrangements for online safety and safeguarding.

An especially important point for Abbey is that the DfE standard expressly recommends blocking technologies such as VPNs and proxy services, while also requiring schools to consider BYOD (**B**ring **Y**our **O**wn **D**evice) devices and the effectiveness of their filtering arrangements.

Produced by:	JKS	Date:	05/12/2024	Checked by:	JKS	Date:	10/11/2026	Approved by:	MN	Date:	10/11/26

Monitoring and Review
• This policy will be subject to continuous monitoring, refinement and audit by the Principal. • The Principal and Welfare Manager will undertake a formal annual review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.
• The next official date for review is **November 2027**

Introduction

Virtual Private Networks (VPNs) are software platforms which allow the user to route internet traffic through a remote server. Some VPN services can make it appear that the user is accessing the internet from a different country and may be used to get around content blocks on video streaming services or to access websites which may be blocked in a country of residence. VPNs can also have legitimate privacy and security uses. However, students who use unauthorised VPNs can bypass the College's web filter and other network security measures, which may remove or weaken protections intended to prevent access to harmful or inappropriate content and to identify safeguarding concerns.

Students are therefore not allowed to use VPNs whilst at the College, except where the College has given prior written authorisation for a specific educational, accessibility or technical purpose. This policy explains how potential VPN use by students is managed.

The College's approach forms part of its wider safeguarding and online safety arrangements. It should be read alongside the College's Safeguarding and Child Protection Policy, Online Safety Policy, Acceptable Use requirements, Behaviour and Discipline arrangements, and relevant privacy information.

This policy will be reviewed periodically to ensure its effectiveness and alignment with evolving technological advancements, safeguarding risks and student needs. Any such changes will be in accordance with applicable statutory guidance, Department for Education guidance and the Independent Schools Inspectorate framework.

The Purpose of this Policy is:

This policy outlines the College's stance on the use of Virtual Private Networks (VPNs) by students on the College premises or using College-issued devices. The goal is to ensure a safe and secure online environment for all students.

The policy also explains the circumstances in which the College may investigate suspected circumvention of its filtering and security arrangements, how concerns will be reported, and how any response will be managed fairly and proportionately.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

Policy

1. Prohibition of VPN Use:

- Students are strictly prohibited from using, installing, attempting to use or enabling unauthorised VPNs on the College premises or on College-issued devices. This includes personal devices brought onto the College grounds.
- The prohibition applies whether a student is connected to the College's Wi-Fi or network, using a College-issued device on another internet connection, or using a personal device on the College premises. Students must not use a VPN, proxy, anonymising service, unauthorised browser extension, DNS or other technical method to bypass College filtering, monitoring or security controls.
- The use of VPNs to bypass College-implemented internet filters or security measures is strictly forbidden.
- Students must not attempt to disable, alter, evade or interfere with filtering, monitoring, device-management, firewall or other security settings. They must not install software or change device settings for the purpose of avoiding College controls.
- At the beginning of each College year, a two-week amnesty is provided to all students to remove any VPNs they have installed or to speak to the College's IT service provider for help with removal. During this period, students should seek assistance promptly and disclose any VPN applications or related settings that they are unsure how to remove.
- Students must comply with reasonable instructions from College staff or the IT service provider concerning the removal or disabling of unauthorised VPN applications or services.
- The College recognises that some VPN technologies have legitimate uses. Such uses do not provide an automatic exemption from this policy. Students must obtain prior written authorisation before using any VPN or similar service on the College premises or with a College-issued device.
- The College's filtering and monitoring arrangements may apply to College-managed devices both on and off site. Students must not attempt to circumvent those arrangements when using College-issued devices away from the College.

2. Rationale:

- College internet filters and security measures are in place to protect students from harmful content, cyber threats, and inappropriate online activity.
- VPN use can compromise the College's ability to filter, monitor and respond to students' online behaviour and safeguarding concerns.
- Bypassing College filters can expose students to risks, including malware, phishing attacks, and access to harmful content.
- The College has safeguarding responsibilities to take appropriate steps to protect children from online harm. Department for Education statutory guidance, including Keeping Children Safe in Education (KCSIE), expects schools and colleges to have appropriate filtering and monitoring arrangements.
- The Department for Education's Filtering and Monitoring: Core Standard specifically identifies VPNs, proxy services and other technologies that allow users to get around filtering as matters that schools and colleges should address through their technical arrangements.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

- No filtering or monitoring system is completely effective. The College therefore uses a combination of technical safeguards, appropriate supervision, education and clear reporting procedures. A VPN prohibition is one element of this wider approach and does not replace those other measures.
- The College's arrangements should be appropriate to the age, needs and risk profile of its students, and should support legitimate teaching and learning without unreasonably restricting educational access.

3. Consequences of Violation:

Violation of this policy may result in disciplinary action, including but not limited to:

- Warning or reprimand
- Restriction of internet access on College devices
- Removal of unauthorised applications or configuration changes, where this can be done lawfully and safely
- Parental notification, where appropriate and consistent with the student's age, safeguarding needs and the College's policies
- Suspension or exclusion, in severe cases, in accordance with the College's Behaviour and Discipline Policy and applicable requirements
- The response will take account of the seriousness and circumstances of the incident, whether the student deliberately sought to access harmful or prohibited material, whether there has been repeated or deliberate circumvention, the student's age and understanding, and any relevant additional needs or vulnerabilities.
- Where a concern indicates possible exposure to harmful or illegal content, exploitation, radicalisation, cyberbullying, threats or other safeguarding risks, it will be referred promptly to the Designated Safeguarding Lead (DSL) and managed in accordance with the College's safeguarding procedures. Disciplinary action will not replace or delay safeguarding action.
- Students should report accidental access to a VPN, proxy or other circumvention service, or any concern about online content, to a member of staff. Prompt and honest reporting will be taken into account when the College considers its response.
- Any investigation or action will be handled fairly and proportionately, with appropriate regard to the College's safeguarding, behaviour, complaints and data protection procedures.

4. Exception for Authorised Use:

- In rare cases, the College may authorise the use of VPNs for specific educational purposes under strict supervision and with prior approval. Such instances will be documented and monitored closely.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

Additional Considerations

- Educational Awareness: The College will provide educational resources to students and parents about the risks associated with VPN use, the importance of adhering to this College policy, safe and responsible internet use, and how to report online safety concerns. This may be addressed through induction, tutorials, assemblies or the relevant PSHE/online safety curriculum.
- Technological Measures: The College will continue to implement and update technological measures to detect and mitigate VPN usage. In consultation with its IT service provider, the College will consider appropriate system-level controls to block VPNs, proxy services and other known methods of bypassing filtering.
- Filtering and Monitoring Review: The College will review its filtering and monitoring provision at least once every academic year, and sooner where there is a significant safeguarding incident, change in working practice, introduction of new technology, material software update or change to network or device configuration. The review will consider whether VPN and proxy controls remain effective.
- Responsibilities: The College will make clear who is responsible for filtering and monitoring at senior leadership level, the DSL's safeguarding oversight, and the technical responsibilities of the College's IT support provider. These roles will work together to review provision, respond to alerts and concerns, and report significant issues through the College's governance and management arrangements.
- Personal Devices and BYOD: The College will consider the filtering and monitoring arrangements applying to personal devices that connect to the College network. Students must not use personal hotspots, portable Wi-Fi, proxy services or other connections to evade College filtering. Where personal devices are permitted to connect to the College network, appropriate network separation and controls will be applied where technically available.
- Off-site Use of College Devices: College-issued devices remain subject to College requirements when used away from the premises. Students must not disable or circumvent installed filtering, monitoring or security controls. Students and parents should understand that the College's ability to apply network-level controls may differ when a device is not connected to the College network.
- Privacy and Data Protection: Filtering and monitoring must be operated lawfully, fairly, transparently and proportionately, in accordance with the UK GDPR, the Data Protection Act 2018, as amended, and the Data (Use and Access) Act 2025 where applicable. The College's privacy information will explain, as appropriate, what activity is monitored, why it is monitored, who may access alerts or reports and how long relevant information is retained. Access to monitoring information will be restricted to authorised staff and service providers with a legitimate role.
- Records and Incident Response: Relevant VPN or filtering incidents, technical checks, exceptions and resulting actions will be recorded where appropriate. Safeguarding concerns will be referred to the DSL. Technical failures or suspected attempts to interfere with College systems will be referred to the appropriate senior leader and IT support provider.
- Staff and Provider Awareness: Relevant staff and the College's IT service provider will be made aware of their responsibilities for reporting and responding to filtering or monitoring concerns. Staff should report suspected bypassing, unexpected access to blocked material, failures of filtering, or any technical issue that may create a safeguarding risk.
- Educational Access and Accessibility: The College will consider legitimate educational, accessibility or technical requirements when reviewing a request for an exception. Any approved

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

arrangement must be risk-assessed, time-limited where appropriate and documented; it must not compromise essential safeguarding protections.

Summary

VPN use by College students is prohibited because it can enable students to bypass the College's web filter and other security measures, thereby weakening protections intended to safeguard students and the College network. There are various consequences (depending on the severity of the situation) for students found using VPNs – including suspension or exclusion in severe cases. The College may authorise the use of VPNs for specific educational purposes under strict supervision and with prior approval. Students and their parents will be provided with educational materials so that they understand the importance of adhering to this College policy.

The College will support this prohibition through appropriate filtering and monitoring, annual review, technical controls, staff awareness and clear safeguarding and reporting procedures. Any monitoring will be undertaken in accordance with the College's data protection and privacy arrangements. By adhering to this policy, students contribute to a safer and more secure online learning environment.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026