

Westminster Tutors



Online Safety Policy
2026-2027

Contents

1. Introduction	1
2. Scope.....	1
3. Legal Status	1
4. Aims.....	2
5. Rationale	2
6. Roles and responsibilities	3
7. Breadth of Online Safety Issues:	6
8. Cyberbullying	8
9. Online Sexual Harassment	9
10. Technology and Prevent Duty.....	10
11. Assessing Risks Online.....	11
12. Phishing and Pharming	11
13. Protecting Personal Data	12
14. Acceptable use of the Internet in the college.....	12
15. How the college will respond to issues of misuse	13
16. Training	15
17. Remote Learning:.....	15
18. Monitoring arrangements.....	16
19. Links with other Policies and Procedures	16
20. Liability of the College.....	16
21. Monitoring and Review:.....	16

1. Introduction

- 1.1 In an increasingly digital world, where technology plays a pivotal role in education and communication, ensuring our students' safety and wellbeing is paramount. This Online Safety policy guides our school community—students, teachers, parents/guardians, staff, and teachers—towards fostering a secure and responsible online environment. By equipping our students with the knowledge, skills, and tools necessary to navigate the digital landscape safely, we aim to empower them to make informed decisions, build positive digital footprints, and become responsible digital citizens. This policy outlines our commitment to online safety, the measures we have implemented, and the collaborative efforts required to promote a culture of digital respect, awareness, and resilience.

2. Scope

- 2.1 All who work, volunteer, or supply services to our college have an equal responsibility to understand and implement this policy and its procedures within and outside of regular college hours, including activities away from college. All new teachers, employees, and volunteers must state that they have read, understood, and will abide by this policy and its procedural documents, and confirm this during their induction; continuing staff and teachers must do so annually through the annual declaration form.

3. Legal Status

- 3.1 This Online Safety Policy complies with ISI's Private Further Education standards framework and Keeping Children Safe in Education 2026, as applicable to private further education colleges. It also follows the Department for Education's current Filtering and Monitoring core standard, which sets out its recommended approach to meeting safeguarding expectations. Westminster Tutors reviews its filtering and monitoring provision at least once each academic year, and sooner when changes or identified risks require it.
- 3.2 The following legislation and guidance have been consulted in the construction of this Online Safety policy:
- [Data Protection Act 2018 \(legislation.gov.uk\)](https://legislation.gov.uk)
 - [Keeping children safe in education - GOV.\(www.gov.uk\)](https://www.gov.uk)
 - [Working together to safeguard children - GOV.UK \(www.gov.uk\)](https://www.gov.uk)
 - [Human Rights Act 1998 \(legislation.gov.uk\)](https://legislation.gov.uk)
 - [Regulation of Investigatory Powers Act 2000 \(legislation.gov.uk\)](https://legislation.gov.uk)
 - [Computer Misuse Act 1990 \(legislation.gov.uk\)](https://legislation.gov.uk)
 - [Police and Justice Act 2006 \(legislation.gov.uk\)](https://legislation.gov.uk)
 - [Prevent duty guidance: for further education institutions in England and Wales.](https://www.gov.uk)
 - [Obscene Publications Act 1959 \(legislation.gov.uk\)](https://legislation.gov.uk)
 - [Protection of Children Act 1978 \(legislation.gov.uk\)](https://legislation.gov.uk)
 - [Criminal Justice Act 2003 \(legislation.gov.uk\)](https://legislation.gov.uk)

4. Aims

4.1 Westminster Tutors' Online Safety policy aims to:

- Educate and guide students on the risks of harmful online challenges, hoaxes, and viral content, supporting their ability to recognise and respond safely to such material.
- Develop robust processes to ensure the online safety of students, staff and teachers, volunteers, proprietors, and parents or guardians, including managing risk from emerging technologies such as AI.
- Deliver a practical approach to online safety, which empowers us to protect and educate the college community about technology use.
- Establish precise mechanisms to identify, intervene and escalate an incident where appropriate, including with remote education, such as lessons delivered online.

4.2 This Online Safety Policy should be read alongside the College's Safeguarding and Child Protection Policy, which sets out the overarching framework for safeguarding at Westminster Tutors. Online safety is an integral part of this framework, and all incidents or concerns will be managed per the College's safeguarding procedures.

5. Rationale

5.1 The college's Leadership Team has authorised this Online Safety policy and addresses its response to promoting a safe and tolerant student environment. Online safety is a running and interrelated theme when devising and implementing our more comprehensive college policies and procedures, including our Safeguarding & Child Protection Policy and Preventing Extremism and Tackling Radicalisation Policy. We consider how to promote online safety while developing our curriculum through staff and teacher training and parental engagement. Technology use is ubiquitous in people's lives, including for students, staff and teachers in education. This policy gives a broad overview of how the college will attempt to ensure that students are not exposed to material that may put them at risk. The college has also produced specific policy guidance documents on the acceptable use of technology for students, staff, and teachers.

5.2 Educational establishments should provide a safe environment for students to learn and work in, primarily when online. Filtering and monitoring are essential to safeguard students from potentially harmful and inappropriate online material.

5.3 The Proprietor retains overall strategic responsibility for filtering and monitoring. The Principal, as DSL, oversees these arrangements, supported by the Pastoral Coordinator, as DDSL. The Principal manages the college network.

5.4 The Principal and Pastoral Coordinator should:

- Procure and maintain an appropriate system.
- Identify risk issues (age of students, SEND issues, EAL, PSHE, RSE, County Lines, BYOD, etc.)
- Carry out reviews.
- Carry out checks.

- 5.5 The system should be robust and block harmful content without affecting teaching and learning unreasonably.
- 5.6 The filtering provider MUST block access to illegal content, including child sexual abuse material.
- 5.7 The DSL oversees filtering and monitoring. The DDSL reviews aggregate OpenDNS domain reports weekly and reports trends and actions to SLT. Close supervision is the main monitoring method. Technical monitoring covers the college network only, does not identify individual users from these reports and does not cover separate mobile data or off-site personal devices. Urgent concerns are reported immediately to the DSL or DDSL. Staff and students must use the college Wi-Fi for college work while on site.
- 5.8 The following is a list of possible risks students may face in their access to technology:
- Access to illegal, harmful, or inappropriate images or content.
 - The risk of being subject to grooming by those whom they contact on the internet.
 - Inappropriate and unsafe communication with strangers.
 - Cyberbullying.
 - Access to pornographic material.
 - Access to extremist material that could lead to the radicalisation of students.
 - Access to unsuitable video or gaming sites.
 - Sites that encourage gambling.
 - Illegal downloading of material that breaks copyright laws.
 - Unauthorised access to/loss of/sharing of personal information.
- 5.9 The above risks can be realised through a wide range of technologies, including:
- E-mail.
 - Smart devices, i.e., watches, phones, tablets, laptops, etc.
 - The Internet (web).
 - Social networking sites: Twitter, YouTube, Facebook, etc.
 - Gaming sites.
 - Blogs, instant messaging, chat rooms, message boards, and virtual learning environments.
 - Webcams, video hosting sites.
 - Photography.
 - Artificial Intelligence.

6. Roles and responsibilities

- 6.1 The Principal is responsible for ensuring the online safety of the college community. Our Pastoral Coordinator will take operational responsibility for online safety in the college. However, overall responsibility remains with the Principal to ensure the policy is enforced and that the necessary checks, filters, and monitoring are in place. The college's responsibility is to ensure that students are safe from cyberbullying within and outside the college community and that appropriate steps are

taken if an incident occurs. During regular meetings, the senior leadership team will also review online safety and the college's acceptable use of technology.

- 6.2 The Principal, as designated safeguarding lead (DSL), leads on online safety, supported by the Pastoral Coordinator, as DDSL. The Principal and senior leadership team are responsible for ensuring staff receive appropriate training, understand the relevant guidance and complete the required declarations. Digital communication with students must remain professional and use official college communication systems. In addition, we must embed online safety in all aspects of the curriculum and other college activities. Students should read, understand, and sign the online safety guidance notes. Parents will be copied on student guidance notes.
- 6.3 Under the direction of our Principal, our Pastoral Coordinator will have a specific duty of care to ensure that suitable controls and filters are in place and that the system is secured and risk-assessed based on college policies.
- 6.4 The Principal manages the college network and oversees the following arrangements:
- All users have clearly defined access rights to the college IT systems.
 - Servers, wireless systems, and cabling are securely located, physically protected, and have access restrictions.
 - All workstations are protected with up-to-date antivirus software.
 - Personal or student data cannot be sent over the Internet or taken off the college site unless safely encrypted.
 - All users are provided with a username and password.
 - Regular reviews of the network system are conducted to examine vulnerabilities and risks.
 - Staff and teachers must take and use student photographs only for authorised college purposes and in accordance with the Data Protection Policy and privacy notices. Where the college requires written permission for a photograph's intended use, this must be obtained from the student if they are 18 or over, or in accordance with the college's procedures for students under 18.
 - Staff, teachers, and students cannot publish images of others without their permission.
 - Students should be fully aware of their responsibilities and limitations regarding images on social media by reading the student guidance notes.
 - Sensitive personal data should be encrypted using password protection before being sent electronically.
 - Staff and teachers must not include any defamatory comments in any emails.
 - Staff and teachers cannot electronically communicate with students inside or outside the college unless they use the designated college system, and all communications are subject to inspection and review.
 - The use of social networking sites within the college is only allowed in appropriately controlled situations and in support of legitimate curriculum activities.
 - Students, staff, and teachers must report any inappropriate material about them or others online, which could bring the college into disrepute.

- 6.5 The proprietor retains overall strategic responsibility for online safety and filtering and monitoring. The Principal, as designated safeguarding lead (DSL), oversees implementation of this policy, supported by the Pastoral Coordinator, as DDSL. The Principal reports relevant findings from online safety, filtering, and monitoring reviews to the proprietor. The Governance Advisory Board may advise on and review these arrangements, but the proprietor retains responsibility. The senior leadership team will:
- Ensure that they have read and understand this policy.
 - Agree and adhere to the terms of the acceptable use agreement (to be signed by all staff and teacher members) of the college's IT systems and the internet.
- 6.6 The Principal and Pastoral Coordinator are responsible for ensuring that staff and teachers understand this policy and that it is being implemented consistently throughout the college. The Principal, who is the DSL, takes lead responsibility for online safety in college, in particular: Contact roles: Principal/DSL — Sean Doherty; Pastoral Coordinator/DDSL — Monika Loewy. The Chair of the Governance Advisory Board is the designated person for concerns about the Principal/DSL, with the Proprietor as fallback; current contact details are in the Safeguarding and Child Protection Policy.
- Support teaching staff and teachers in understanding this policy and ensure it is implemented consistently throughout the college.
 - Working with other staff and teachers, as necessary, to address any online safety issues or incidents.
 - Ensuring that online safety incidents are logged and handled appropriately per this policy.
 - Ensuring that cyberbullying incidents are logged and handled appropriately following the college's Behaviour Policy.
 - Updating and delivering staff and teacher training on online safety.
 - Liaising with other agencies or external services if necessary.
 - Providing regular reports on online safety in college to the GAB.
 - This list is not intended to be exhaustive.
- 6.7 The Principal oversees the following online safety and technical arrangements:
- Putting in place appropriate filtering and monitoring systems, which are updated regularly and keep students safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material.
 - Ensuring that the college's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
 - Overseeing weekly aggregate OpenDNS report reviews by the DDSL and reviewing filtering and monitoring provision at least once each academic year, and sooner when changes or identified risks require it.
 - Blocking access to potentially dangerous sites and, where possible, preventing downloading of potentially harmful files.
 - Ensuring that online safety incidents are logged and handled appropriately per this policy.

- Ensuring that cyberbullying incidents are handled appropriately per the college's Behaviour Policy.
- This list is not intended to be exhaustive.

6.8 All employees, independent teachers, other contractors and volunteers are responsible for the following:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing to and adhering to the acceptable use of the college's IT systems and the internet, and ensuring that students follow the college's terms on the acceptable use agreement.
- Working with the DSL as the Prevent Lead to ensure that online safety incidents are logged and handled appropriately per this policy.
- Ensuring that cyberbullying incidents are handled appropriately per the college's Behaviour Policy.
- This list is not intended to be exhaustive.

6.9 Parents are expected to:

- Notify a member of staff and teachers, a senior leader, or the Principal of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms of the acceptable use agreement for the college's IT systems and internet.
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
 - [Parents and Carers - UK Safer Internet Centre](#)
 - [Help & advice | Childnet](#)
 - [Parents and carers | CEOP Education \(thinkuknow.co.uk\)](#)
 - [Keeping children safe online | NSPCC](#)

6.10 Visitors and community members who use the college's IT systems or the Internet will be made aware of this policy when relevant and are expected to read and follow it. If appropriate, they will agree to the acceptable use agreement terms.

7. Breadth of Online Safety Issues:

7.1 We classify the issues within online safety into four areas of risk:

- **Content:** exposure to illegal, inappropriate, or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example, student-to-student pressure, commercial advertising, and adults posing as children or young adults to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and pornography, sharing other graphic images and online bullying)

- **Commerce** - risks such as online gambling, inappropriate advertising, phishing, and financial scams.
- 7.2 These issues must be managed by reducing availability, restricting access, and promoting safe and responsible use.
- 7.3 The widespread use and availability of technology and social networks present opportunities and risks. This policy sets out what practices are deemed acceptable and unacceptable. We do not intend to prevent anyone from using technology or social media, but to ensure that, when they do, they do so in a way that protects themselves, their peers, and the college's reputation.
- 7.4 We accept that students regularly bring their own devices into college, which can enhance the learning experience if used sensibly. Students must, however, be guided by their class teacher about the appropriate use of tablets and laptops in lessons and respect and comply with their views.
- 7.5 Although the college cannot control the use of social media off-site and out-of-hours, should any material come to light that is defamatory, abusive, or offensive or involves bullying and contravenes the ethos and values of the college, we will take steps to investigate, and where necessary impose sanctions, suspensions, or exclusion. Westminster Tutors' advice to students is simple: enjoy the benefits of technology and social media, but respect college policy, respect your peers, and think before you post or send material or images.
- 7.6 Students will be taught about online safety as part of the curriculum, including:
- Understand various ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
 - Recognise inappropriate content, contact, and conduct, and know how to report concerns.
 - How to report a range of concerns.
 - The safe use of social media and the internet will also be covered in other relevant subjects.
 - Online safety is taught through Student Discussion, mentoring and relevant teaching. The college may invite speakers to support this education.
 - We recognise that abuse between students can occur online, including child-on-child abuse where those involved are under 18. We teach students to recognise warning signs, report concerns and seek help if they experience or witness online sexual harassment or other abuse.
- 7.7 When accessing the internet, individuals are especially vulnerable to several risks which may be physically and emotionally harmful, including:
- Access to illegal, harmful, or inappropriate images.
 - Cyber-bullying.
 - Access to, or loss of, personal information.
 - Access to unsuitable online videos or games.
 - Loss of personal images.
 - Inappropriate communication with others.
 - Illegal downloading of files.
 - Exposure to explicit or harmful content, e.g., involving radicalisation.

- Plagiarism and copyright infringement.
 - Sharing the personal information of others without the individual's consent or knowledge.
- 7.8 Staff and teachers should be vigilant in lessons where students use the Internet. If staff and teachers allow mobile devices in their classes, they must ensure they are used in line with college policy.
- 7.9 The college will raise parents' awareness of internet safety in letters or other communications home and via the website. The college will also share this policy with parents via the website. If parents have any queries or concerns about online safety, they should first raise them with the Principal or Pastoral Coordinator.

8. Cyberbullying

- 8.1 Cyberbullying occurs online, through social networking sites, messaging apps, or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the college's Behaviour Policy.) A serious one-off online incident, including the continuing circulation of harmful content, will be addressed promptly even where it does not meet the definition of repeated bullying. The Anti-Bullying Policy applies alongside this policy.
- 8.2 To help prevent cyberbullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure students know how to report incidents and are encouraged to do so, including when they witness it rather than being the victim(s). The college will actively discuss cyberbullying with students, explaining why it occurs, the forms it may take, and the consequences. Cyberbullying will be discussed through Student Discussion, mentoring and relevant teaching. Teaching staff and teachers are also encouraged to find opportunities to cover cyberbullying through aspects of the curriculum. This includes personal, social, health and economic (PSHE) education and other subjects where appropriate.
- 8.3 As part of safeguarding training, all staff and teachers, proprietors, and volunteers (where appropriate) receive training on cyberbullying, its impact, and ways to support students.
- 8.4 The college also sends information/leaflets on cyberbullying to parents so that they know the signs, how to report it and how they can support children who may be affected.
- 8.5 In the case of a specific cyberbullying incident, the college will follow the processes set out in its Behaviour Policy. Where illegal, inappropriate, or harmful material has been spread among students, the college will use all reasonable endeavours to ensure the incident is contained. The Principal, acting as the DSL and Prevent Lead, will consider whether to report the incident to the police if it involves illegal material and will work with external services if necessary.
- 8.6 Concerns about a device or its contents must be referred immediately to the DSL or DDSL. Any examination, retention or deletion must have a lawful basis and follow the Safeguarding and Child Protection Policy; this policy grants no search power. Staff and teachers must not investigate, copy, share or delete suspected child sexual abuse imagery. The DSL will follow UKCIS guidance on sharing nudes and semi-nudes, under which viewing imagery is considered only in exceptional circumstances, and seek police advice where appropriate. Complaints about the handling of a device will be dealt with under the college's complaints procedure.

9. Online Sexual Harassment

- 9.1 Online sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviour and provide an environment that may lead to sexual violence. Online sexual harassment includes:
- Non-consensual sharing of sexual images and videos and sharing sexual pictures and videos (often called sexting).
 - Inappropriate sexual comments on social media; exploitation; coercion and threats.
- 9.2 Online sexual harassment may be standalone or part of a broader pattern of sexual harassment or sexual violence. All cases or allegations, online or offline, are unacceptable and will be addressed under the Safeguarding and Child Protection Policy. Child-protection procedures apply to students under 18. Concerns involving students aged 18 or over follow the policy's adult safeguarding and support arrangements, with appropriate police or adult social care referrals where required. Where an incident also affects a child, child-protection procedures apply to that child.
- 9.3 Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection with offline incidents) can introduce several complex factors. These include the potential for the incident to span several social media platforms and services, and for things to move from platform to platform online. They can also extend the impact beyond the college's local community (e.g., images or content shared around neighbouring colleges/colleges). They can marginalise and exclude a victim (or alleged perpetrator) in both online and offline communities. There is also the strong potential for repeat victimisation if abusive content continues to exist somewhere online. Online concerns can be incredibly complicated. Support is available at:
- The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. It provides expert advice and support for college staff and teachers about online safety issues and when an allegation is received.
- 9.4 If sexual images or videos of a student are shared online, the Principal, acting as designated safeguarding lead (DSL), will assess the safeguarding concern and support the student in reporting the material through an appropriate removal service or platform. Images depicting a child may be reported to the Internet Watch Foundation (IWF); a student under 18 may also be supported to use Childline and the IWF's Report Remove service. The DSL will consider a referral to the police or children's social care where appropriate.
- 9.5 The impact on a young person of IT-based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension: a visual record of the abuse. IT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response are recognising a situation where a child is suffering or is likely to suffer a degree of physical, sexual, or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff and teachers) working with students, adults, and families will be alerted to the possibility that:
- A child may already have been/is being abused, and the images are distributed on the Internet or by mobile telephone.

- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve showing the child offensive photos.
 - An adult or older child may view and download child sexual abuse images.
- 9.6 Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the college and may constitute a criminal offence. The college will treat incidents of sexting (both sending and receiving) as a safeguarding issue. Students concerned about images obtained, sent, or forwarded should ask any staff member or teacher for advice.
- 9.7 Adults must not access, create, possess or share child sexual abuse images. Concerns about the Principal/DSL, at any level, must be reported to the Chair of the Governance Advisory Board as the designated person, or to the Proprietor if the Chair is unavailable or conflicted, in accordance with the Safeguarding and Child Protection Policy. Other safeguarding concerns must be reported immediately to the DSL or DDSL. The college will involve the police and Local Authority Designated Officer (LADO) as required and consider any employment or barring action in accordance with the relevant procedures.
- 9.8 Adults must not use college equipment to access pornography or bring pornographic material into the workplace on personal devices. They must take reasonable steps to prevent students from being exposed to inappropriate images or links. Any concern involving suspected child sexual abuse imagery or inappropriate conduct by an employee or independent teacher must follow the reporting routes above. The Principal will follow the college's safeguarding procedures and contact the police, children's social care or the LADO as appropriate. Staff must not investigate or copy suspected child sexual abuse imagery themselves.

10. Technology and Prevent Duty

- 10.1 As part of an integrated policy linked to the Prevent strategy, the college also must ensure that students are prevented and protected from the risk of being radicalised through access to extremist propaganda, e.g., from ISIL. The college must promote British values through the curriculum, SMSC, and RSE. Teachers must also be aware of their responsibility to monitor and report serious concerns about a student's use of, or access to, inappropriate material that undermines British values and tolerance of others. The college's network and facilities must not be used for the following activities:
- Accessing or downloading pornographic material.
 - Gambling.
 - Accessing sites or social media channels that promote extreme viewpoints and radical propaganda.
 - Soliciting for personal gain/profit.
 - Revealing or sharing proprietary or confidential material.
 - Purporting to speak on behalf of the college without authorisation. Nothing in this policy prevents lawful complaints, safeguarding reports or protected disclosures.
 - Posting indecent or humiliating images or remarks/proposals.

11. Assessing Risks Online

- 11.1 We will take reasonable precautions to prevent access to inappropriate online material, including filtering, monitoring, staff supervision and online safety education. These measures cannot guarantee that unsuitable material will never be accessed. We will respond to concerns or incidents under our safeguarding and behaviour procedures and fulfil our legal responsibilities.
- 11.2 The college's infrastructure does not govern developing technologies, such as mobile phones with Internet access that can bypass security and filtering measures that are or could be deployed. We recognise the additional risks this has for our students, who could have unsupervised access to the internet when using their own devices in their free time. To address this, the college works with students across our age range to ensure they are clearly educated about social media and internet use risks, and regularly monitors device usage as appropriate.
- 11.3 We will audit IT use to establish whether the Online Safety policy is sufficiently robust and whether its implementation is appropriate and effective.
- 11.4 Methods to identify, assess and minimise risks will be reviewed regularly.
- 11.5 The Principal, as DSL, supported by the DDSL, will assess safeguarding and security risks before introducing new technology for college use. Access to college systems will be limited to authorised users according to their roles. Dashboard and monitoring-log access is limited to the DSL and DDSL. The Principal manages the college network; no external administrator or contractor has access. Visitors may be given access to the filtered guest Wi-Fi network.
- 11.6 Westminster Tutors ensures appropriate IT filters and monitoring systems are in place to safeguard students from potentially harmful and inappropriate material online without unreasonable "over-blocking."
- 11.7 The college recognises that students may circumvent certain safety precautions by using mobile data on their devices. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management, additional staff, and teacher/student training.

12. Phishing and Pharming

- 12.1 A phishing email usually contains a link with directions asking the recipient to click on it. Clicking the link transports the email recipient to an authentic-looking, albeit fake, web page. The target is asked to enter information such as a username and password or additional financial or personal data.
- 12.2 The perpetrator who orchestrates the phishing scheme can capture this information and use it to further criminal activity, like theft from a financial account and similar illegal activity.
- 12.3 The college has no intention of changing its financial information; therefore, never accept an email pretending to be the college's accounts department with a link.

Top tips:

- Never click on hyperlinks in an email from an unknown sender; instead, manually type the URL into the web browser.

- Never enter sensitive information in a pop-up window except on sites that an individual knows to be trustworthy.
- Before entering confidential information, check that the website address is the one you intended to visit and that the connection uses HTTPS. HTTPS protects the connection but does not prove that the website or organisation is genuine. If a link or request seems suspicious, contact the organisation using details you have obtained independently.
- Access personal and financial information only from a computer or device you trust to be free from trojans and keyloggers.
- Education on phishing and pharming attacks—it is crucial to stay abreast of phishing scams and the technology and techniques designed to prevent them. Many reliable educational resources online help people prevent phishing attacks.
- Report phishing and pharming to the Principal.

Characteristics of a strong password

- At least eight characters – the more characters, the better.
- A mixture of both uppercase and lowercase letters.
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?].

13. Protecting Personal Data

- 13.1 Personal data will be collected, used, stored, shared and deleted in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Where the law permits or requires it, the college may share relevant personal data with the police or other appropriate authorities.

14. Acceptable use of the Internet in the college

- 14.1 All students, parents, staff and teachers, volunteers, and proprietors are expected to sign an acceptable use agreement before using the college's IT systems and the internet.
- 14.2 Visitors must read and agree to the college's acceptable use terms if relevant.
- 14.3 Use of the college's internet must be for educational purposes or to fulfil the duties of an individual's role. Monitoring combines close supervision with weekly review of aggregate OpenDNS domain reports, as described in section 5. These reports do not identify individual users or prove deliberate visits.
- 14.4 Students may bring mobile devices into the college, but are not permitted to use them without teacher permission during:
- Lessons.
 - Personal Tutor time.
 - Clubs, sessions on the premises, or any other activities organised by the college.
- 14.5 Students' use of mobile devices in the college must align with the acceptable use agreement.

- 14.6 Any student's breach of the acceptable use agreement may trigger proportionate action under the Behaviour Policy. Any request to hand over a device, examination or retention must have a lawful basis and follow the safeguards in section 8.
- 14.7 Staff and teachers using work devices outside the college: Staff and teachers using a work device outside the college must not install any unauthorised software or use the device in any way that would violate the college's terms of acceptable use agreement.
- 14.8 Staff and teachers must ensure that their work device is secure and password-protected with a strong password, as well as their online login details to Google, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside the college. Any USB devices containing data relating to the college must be encrypted. If staff and teachers have any concerns over the security of their device, they must seek advice from the Principal. Work devices must be used solely for work activities.

15. How the college will respond to issues of misuse

- 15.1 Where a student misuses the college's IT systems or internet, we will follow the procedures set out in the Behaviour Policy. The action taken will depend on the specific incident's circumstances, nature, and seriousness, and will be proportionate.
- 15.2 Employee misconduct is addressed under employee procedures. Concerns about independent teachers are addressed under the applicable teacher agreement and safeguarding procedures, without treating teachers as employees. The response will depend on the circumstances, nature and seriousness of the incident. The college will consider whether incidents involving illegal activity, content or otherwise serious concerns should be reported to the police.
- 15.3 If a college community member breaches any terms in our policy and guidance documents, sanctions can be applied. In severe cases, the appropriate authority will be notified. This will be exercised on a case-by-case basis and proportionately. Students may face action under the Behaviour Policy; employees and independent teachers are subject to the distinct procedures described above.
- 15.4 Members of the college community must follow these rules:
- Do not disclose your username or password to others.
 - Do not read another person's email without permission.
 - Do not photograph another student, or post or share another person's image, without permission.
 - Do not delete an image or file that may be evidence of a safeguarding concern or offence. Refer it to the DSL or DDSL and follow the safeguards in section 8.
 - Do not use college computers for gaming or gambling.
 - Report any accidental download of inappropriate material immediately to a member of the senior leadership team.
 - Use social media during college time only when authorised for college purposes.
 - Switch off or silence and put away mobile phones during lessons and other activities when required, except where educational use is authorised by the teacher. Examination restrictions apply separately.

- Do not obtain unauthorised access to a college network or system.
- Respect copyright and do not present another person's work as your own.
- Do not display or share offensive material or content likely to promote radicalisation.

- 15.5 Breaches will be addressed under the Behaviour Policy, employee procedures or the applicable independent teacher agreement, according to the person's status, with safeguarding procedures and referrals to the police or other authorities applied where appropriate.
- 15.6 Where there are reasonable grounds to suspect that a student's device has been used in connection with an offence or a safeguarding concern, staff must refer the matter to the DSL or DDSL. Any request to hand over a device, examination of its contents or retention of the device must have a lawful basis and follow the college's safeguarding and behaviour procedures. The DSL will involve the police where appropriate.
- 15.7 Students must treat all IT equipment respectfully, not print out lengthy items and not use significant amounts of paper.
- 15.8 The college does allow students to bring in their own devices, but they are only allowed to physically connect to the college system if they have permission from the Principal.
- 15.9 Mobile phone communication between staff, teachers, and students is permissible during visits and field trips, but this will usually be on a college-dedicated mobile.
- 15.10 Students cannot film or record other students or their teacher during or outside class without specific permission, which will generally be in writing for staff and teachers.
- 15.11 Mobiles must be switched off and handed to an invigilator for safekeeping when this request is issued before the announcement of a formal examination.
- 15.12 During lessons, mobile phones must be switched off or silenced and put away unless the teacher authorises their use for an educational purpose. During mocks and formal examinations, students must follow the examination rules and invigilator instructions; teacher permission for classroom use does not override examination restrictions.
- 15.13 Staff and teachers must use approved college channels when communicating with students about college matters. They must not use personal email accounts or personal social media channels for those communications. Students should use the college's designated channels to contact staff and teachers about college matters.
- 15.14 If the Principal has reasonable grounds to suspect inappropriate communication between a member of staff and a student, the concern will be managed under the college's safeguarding and staff conduct procedures. The college may preserve relevant information on its own systems and request that individuals retain relevant communications. Do not take or examine personal devices without a lawful basis. The Principal will seek advice from the LADO or police where appropriate. Concerns about the Principal/DSL, at any level, must be reported to the Chair of the Governance Advisory Board as the designated person, or to the Proprietor if the Chair is unavailable or conflicted, in accordance with the Safeguarding and Child Protection Policy. Other safeguarding concerns must be reported immediately to the DSL or DDSL.

16. Training

- 16.1 As part of their induction, all new staff and teacher members will receive training on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation.
- 16.2 All staff and teachers will receive refresher training at least once each academic year as part of safeguarding training and relevant updates as required (for example, through emails, e-bulletins, and staff and teachers' meetings).
- 16.3 The Principal acting as the DSL and Prevent Lead will undertake child protection and safeguarding training, including online safety, at least every two years. They will also regularly update their knowledge and skills about online safety, at least annually.
- 16.4 Volunteers will receive appropriate training and updates, if applicable. Our Child Protection and Safeguarding policy and the Prevent policy provide more information about safeguarding training.

17. Remote Learning:

- 17.1 These online safety safeguards apply to all approved remote learning, not only emergency closures. Westminster Tutors supports staff, independent teachers and students in accessing learning safely, with particular attention to vulnerable students, in accordance with the Remote Learning Policy.
- 17.2 Staff, teachers and volunteers who interact with students online must remain alert to signs of abuse and safeguarding concerns and report them promptly under the Safeguarding and Child Protection Policy.
- 17.3 Staff, teachers and volunteers will remain alert to signs of abuse or effects on learners' mental health that are safeguarding concerns and act immediately. Concerns must follow the Safeguarding and Child Protection Policy, using child-protection procedures for students under 18 and the adult safeguarding and support arrangements for students aged 18 or over. Referrals to children's or adult social care, or the police, will be made as appropriate.
- 17.4 Online teaching must follow the Staff and Teacher Code of Conduct and the college's requirements for students' acceptable use of technology. Westminster Tutors will use online learning tools and systems in accordance with its Data Protection Policy and privacy notices.
- 17.5 The college will implement additional measures to support parents and students learning from home. This will include specific guidance on which programmes the college expects students to use and how to access these, alongside how students and parents can report any concerns. Advice will also be issued on which staff and teacher members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our college's Remote Learning Policy.
- 17.6 Additionally, the Principal has a duty of care to ensure college community members' safety (including online safety), with the day-to-day responsibility being delegated to the Pastoral Coordinator.
- 17.7 The Principal and Pastoral Coordinator follow the safeguarding reporting procedures for all concerns about an employee or independent teacher, including low-level concerns and allegations. Concerns about the Principal/DSL, at any level, must be reported to the Chair of the Governance Advisory Board as the designated person, or to the Proprietor if the Chair is unavailable or conflicted, in accordance

with the Safeguarding and Child Protection Policy. Other safeguarding concerns must be reported immediately to the DSL or DDSL.

- 17.8 Staff and teachers working remotely should, wherever possible, use their college-issued IT equipment.
- 17.9 However, they may use their computer equipment if it is not practical and follows the college's Data Protection Policy. Staff and teachers are responsible for the security of personal data. They must ensure it is stored securely when using personal or remote systems to maintain confidentiality from other household members.

18. Monitoring arrangements

- 18.1 The DDSL logs behaviour and safeguarding issues related to online safety and reviews aggregate OpenDNS reports weekly. Urgent concerns are reported and acted on immediately rather than waiting for the weekly review.

19. Links with other Policies and Procedures

- Child Protection and Safeguarding policy.
- Prevent policy.
- Behaviour Policy, Anti-Bullying Policy, Curriculum Policy and Remote Learning Policy.
- Employee procedures and applicable independent teacher agreements.
- Data Protection Policy and Privacy notices.
- Complaints Procedure.

20. Liability of the College

- 20.1 The college will consider incidents involving students' use of mobile phones, email or the internet under its relevant policies and applicable law. Nothing in this policy excludes or restricts a legal responsibility or liability that the college cannot lawfully exclude or restrict.

21. Monitoring and Review:

- 21.1 The Principal, as DSL, oversees a review of filtering and monitoring provision at least once each academic year, and sooner when changes or identified risks require it. The DDSL supports the review. Findings and actions are reported to the Proprietor; the Governance Advisory Board may advise on and review these arrangements, while the Proprietor retains responsibility.
- 21.2 Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff and teachers will be informed of the updated/reviewed arrangements, which will be made available in writing or electronically.

Ownership and consultation	
Document author (name)	Sean Doherty, Principal
Audience	
Audience	Principal, college staff and teachers, students, and parents
Version control	
Implementation date	September 2024
Reviewed dates	September 2025 September 2026 15 October 2026 — approved by the Principal
Next Review	September 2027