Westminster Tutors

Online Safety Policy

2023-2024

Contents

1. Introduction

1.1 In an increasingly digital world, where technology plays a pivotal role in education and communication, ensuring our students' safety and well-being is paramount. This Online Safety policy guides our school community—students, teachers, parents/guardians, and staff—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 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 and continuing members of staff 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 upholds guidance and recommendations from the DfE, specifically Keeping Children Safe in Education Part 1, paragraphs 135-148.

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)
- Keeping children safe in education - GOV.UK (www.gov.uk)
- Working together to safeguard children - GOV.UK (www.gov.uk)
- Human Rights Act 1998 (legislation.gov.uk)
- Regulation of Investigatory Powers Act 2000 (legislation.gov.uk)
- Computer Misuse Act 1990 (legislation.gov.uk)
- Police and Justice Act 2006 (legislation.gov.uk)
- Prevent duty guidance: for further education institutions in England and Wales.
- Obscene Publications Act 1959 (legislation.gov.uk)
- Protection of Children Act 1978 (legislation.gov.uk)
- Criminal Justice Act 2003 (legislation.gov.uk)

4. Aims

4.1 Westminster Tutors Online Safety policy aims to:

- Have robust processes to ensure the online safety of students, staff, volunteers, proprietors and parents or guardians.
- Deliver an effective approach to online safety, which empowers us to protect and educate the college community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate.

5. Rationale

5.1 The college's Leadership Team has authorised this Online Safety policy and addresses the college's response to promoting a safe and tolerant environment for its students. 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 we can promote online safety whilst developing our curriculum through staff training and parental engagement. Technology use is ubiquitous in people's lives, which is also true for students and staff within education. This policy gives a broad overview of how the college will attempt to ensure that students are not exposed to material content that may put them at risk. Other specific policy guidance documents have been produced for students and staff concerning the acceptable use of technology.

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 Governing bodies and proprietors must have overall strategic responsibility for filtering and monitoring. The Director of Studies (Pastoral) is the assigned member of the senior leadership team responsible for ensuring these standards are met. The Director of Studies (Pastoral) will work closely with the college's IT technician for specialist technical support.

5.4 Director of Studies (Pastoral) and IT Technician 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 an illegal content, including child sexual abuse material.

5.7 All existing college computers and devices are monitored and checked by the Director of Studies (Pastoral) and IT Technician. While on-site, all staff and students must use the college's WiFi Internet network.

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.

6. Roles and responsibilities

6.1 The Principal, working in conjunction with our IT Technician, is responsible for ensuring the online safety of the college community. Our Director of Studies (Pastoral) will take operational responsibility for online safety in the college. Still, the overall responsibility will fall on the Principal to ensure that 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 their regular meetings, the senior leadership team will also review online safety and the acceptable use of technology in the college.

6.2 The Director of Studies (Pastoral), who is also the DSL, will act as the online safety officer with the assistance of our Data Protection Officer. They, along with the senior leadership team, will also be responsible for staff training and ensure that staff are aware of the guidance notes to staff and have signed them accordingly. Specifically, staff must be mindful that digital communication with students should be professional and only carried out using official communications systems. In addition, online safety must be embedded in all aspects of the curriculum and other college activities. Students should have read, understood, and signed the guidance notes on online safety. Parents will be copied with student guidance notes.

6.3 Under the direction of our Director of Studies (Pastoral), our IT Technician will have a specific duty of care to ensure that suitable controland filters are in place and that the system is secured and risk-assessed based on college policies.

6.4 The Principal should work with the IT Technician and College Administrator to ensure that:

- 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 virus 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 taken to examine vulnerabilities and risks.
- Staff must be careful when taking student images, even if they support educational aims. Any photos taken for educational purposes can only be done with the parents' and students' prior permission (written).
- Staff and students cannot publish images of others without their permission.
- Students should be fully aware of their responsibilities and limitations regarding images over social media by reading the student guidance notes.
- Sensitive personal data should be encrypted using password security before being sent electronically.
- Staff must not include any defamatory comments in any emails.
- Staff 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 support of legitimate curriculum activities.
- Students and staff must report any inappropriate material about them or others online, which could bring the college into disrepute.

6.5 The proprietor and the senior leadership team monitor this policy and hold the Principal and Director of Studies (Pastoral) accountable for its implementation. The proprietor will delegate to the Governance Advisory Board to coordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL). 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 members) of the college's IT systems and the internet.

6.6 The Principal and Director of Studies (Pastoral) are responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the college. The Director of Studies (Pastoral), who is the DSL, takes lead responsibility for online safety in college, in particular:

- Supporting the Principals in ensuring that staff understand this policy and that it is being implemented consistently throughout the college.
- Working with the Principal, IT Technician, and other staff, 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 training on online safety.
- Liaising with other agencies or external services if necessary.

- Providing regular reports on online safety in college to the Principal.
- This list is not intended to be exhaustive.

6.7 The IT Technician and Data Protection Officer are responsible for the following:

- 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.
- Conducting a full security check and monthly monitoring of the college's IT systems.
- Blocking access to potentially dangerous sites and, where possible, preventing downloading 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 staff, including contractors and agency staff, and volunteers, are responsible for the following:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the college's IT systems and the internet and ensuring that students follow the college's terms on 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, 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 acceptable use agreement of thecollege'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 internet will be made aware of this policy when relevant and are expected to read and follow it. If appropriate, they will be expected to 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 togroom 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; and
- **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 responsibleuse.

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. It is not our intention to prevent anyone from using technology or social media, but merely to ensure that when they use these technologies, they do so in a manner 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 offsite 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.

- The college will use assemblies to raise students' awareness of the dangers that can be encountered online and may invite speakers to talk to students.
- We recognise that peer-on-peer abuse can occur online, and to this end, we teach students how to spot early warning signs of potential abuse and what to do if students are subject to sexual harassment online.

7.7 When accessing the internet, individuals are especially vulnerable to several risks which may be physicallyand 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 should be vigilant in lessons where students use the Internet. If staff allow mobile devices intheir classes, they must ensure they are used per college policy.

7.9 The college will raise parents' awareness of internet safety in letters or other communications home and viathe. This policy will also be shared with parents via the website. If parents have any queries or concerns about online safety, these should be raised in the first instance with the Principal or Director of Studies (Pastoral).

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.)

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 that students know how to report incidents and are encouraged to do so, including where they are a witness rather than the victim(s). The college will actively discuss cyberbullying with students, explaining why it occurs, the forms it may take and what the consequences can be. Heads of Year and Personal Tutors will discuss cyberbullying with their students and tutees, and the issue will be addressed in assemblies. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHCE) education and other subjects where appropriate.

8.3 All staff, proprietors, and volunteers (where appropriate) receive training on cyberbullying, its impact, and ways to support students as part of safeguarding training).

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.

8.4 With a specific incident of cyberbullying, the college will follow the processes set out in the college's 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 Director of Studies (Pastoral) acting as the DSL and Prevent Lead will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if necessary.

8.5 College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads, and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm.
- Disrupt teaching.
- Break any of the college rules.

8.6 If inappropriate material is found on the device, it is up to the staff member in conjunction with the Director of Studies (Pastoral) or another member of the senior leadership team to decide whether they should:

- Delete that material.
- Retain it as evidence (of a criminal offence or a breach of college discipline).
- Report it to the police.

8.7 Any searching of students will be carried out in line with the DfE's latest guidance on searching, screening and confiscation guidance. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be handled through 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 of sexual harassment, online or offline, are unacceptable and will dealt with under our Child Protection Procedures.

9.3 Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (eitherin isolation or in connection with offline incidents) can introduce several complex factors. These include the potential for the incident across several social media platforms and services and for things to move from platform to platform online. They also have the potential for the impact of the incident to extend further than the college's local community (e.g., for images or content to be shared around neighbouring colleges/colleges) and for a victim (or alleged perpetrator) to become marginalised andexcluded by 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. Providing expert advice and support for college staff about online safety issues and when an allegation is received.

9.4 If an incident involves sexual images or videos made and circulated online, we will support the victim in removing the images through the Internet Watch Foundation (IWF). The IWF will assess whether the image is illegal per UK Law. The image will be removed and added to the IWF's Image Hash list if it is considered illegal.

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 in that there is 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) 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 makingabusive images. This process can involve the child being shown offensive images.
- 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 incidences of sexting (both sending and receiving) as a safeguarding issue. Students concerned about images obtained, sent, or forwarded should ask any staff member for advice.

9.7 No circumstances will justify adults possessing indecent images of students. Adults who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making, and storing indecent images of students is illegal. If proven, this will lead to criminal investigation and the individual being barred from working with students.

Adults should not use equipment belonging to the college to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the adult's suitability to continue working with students. Adults should ensure students are not exposed to inappropriate images or web links. Where indecent images of students or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) will be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to contaminated evidence, which can lead to criminal prosecution.

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 or access to inappropriate material, which undermines British values and the 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.
- Representing personal opinions about the college.
- Positing indecent or humiliating images or remarks/proposals.

11. Assessing Risks Online

11.1 We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a computer connected to the college network. The college cannot accept liability for any material accessed or any consequences of Internet access.

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 that students are educated clearly about the risks of social media and internet use, alongside regularly monitoring device usage as appropriate.

11.3 We will audit IT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.

11.4 Methods to identify, assess and minimise risks will be reviewed regularly.
The Governance Advisory Board will review and examine emerging technologies for educational benefit, and a risk assessment will be carried out before use in college is allowed. Only people directly employed by the college will be provided access to any college system except for filtered Wi-Fi access.

11.5 Westminster Tutors ensures appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material online without unreasonable "over-blocking."

11.6 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 and additional staff/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 input information like 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 with a link pretending to be the college's accounts department.

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 at those sites that an individual knows to be trustworthy.
- Verify HTTPS on the address bar - whenever a person conveys confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S" confirms that the data is conveyed through a legitimate, secure channel.
- 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 - staying abreast of phishing scams and the technology and techniques designed to prevent them is crucial. A plethora of reliable educational resources exist on the Internet designed to assist a person in preventing phishing attacks.
- Report phishing and pharming to the IT Technician.

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 recorded, processed, transferred, and made available according to the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018. The college recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private in our Online Safety lessons and IT curriculum, including password protection and knowledge about apps and unsecured networks/apps, etc. The college will act responsibly to ensure we have an appropriate level of security protection procedures in place to safeguard systems, staff, and learners, and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

14. Acceptable use of the Internet in the college

14.1 All students, parents, staff, 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 only or to fulfil the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, proprietor, and visitors (where relevant) to ensure they comply with the above.

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 be in line with the acceptable use agreement.

14.6 Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with thecollege's Behaviour Policy, which may result in confiscating their device.

14.7 Staff using work devices outside the college: Staff members 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 must ensure that their work device is secure and password-protected with a strong password, so too 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 them outside the college. Any USB devices containing data relating to the college must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the IT Technician. 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. Where a staff member misuses the college's IT systems, the internet, or a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the specific incident's circumstances, nature, and seriousness. The college will consider whether incidents involving illegal activity, content, or otherwise serious incidents should be reported to the police.

15.2 If a college community member breaches any of the terms in our policy and guidance documents, sanctions can be applied. In severe cases, any offender will be reported to the appropriate authority. This will be exercised on a case-by-case basis and proportionately. Both staff and students will be subject to disciplinary action depending on the action they have taken and its impact on others, the college's reputation, or undermining British values.

15.3 Members of the college community cannot:

- Disclose their password and username to other people.
- Read another person's email without consent.
- Take photographs of other students without their permission.
- Post or share images of other college community members without their full permission.
- Staff must delete specific images if a senior leadership team member requests.
- The college computers cannot be used for gaming or gambling.
- If there has been an accidental download of material that is inappropriate, a senior leadership team member must be informed immediately.
- Use social media during college time.
- Mobile phones must be switched off or silent during lessons and key extracurricular activities, e.g., assemblies and events.
- Knowingly obtain unauthorised access to any part of our network or system through hacking; this is a criminal offence.
- You must respect copyright laws and understand that you cannot copy and paste other people's work and claim it as your own - this is plagiarism.
- Display or distribute/share offensive material, including, but not limited to, racism, sexism, pornography, bullying, homophobic bullying or negative comments, defamation, or images likely to offend others.

Anyone found to have offensive material will be subject to serious disciplinary proceedings, which may result in suspension, exclusion and, in severe cases, involvement of the police or relevant authorities.

- Share or distribute any material that is likely to undermine British values and could radicalise others.

15.4 The college has the right to confiscate and investigate the content of e-equipment if it has serious ground that an offence has occurred, and the Police may become involved for legal reasons.

15.5 Students must treat all IT equipment respectfully, not print out lengthy items and use significant amounts of paper.

15.6 The college does allow students to bring in their own devices, but they are only allowed to physically connect with the college system if they have permission from the IT Technician.

15.7 Mobile phone communication between staff and students is permissible during visits and field trips, but this will usually be on a college-dedicated mobile.

15.8 Students cannot film or record other students or their teacher during or outside class unless with specific permission, which will generally be in writing for staff.

15.9 Mobiles must be switched off and handed to an invigilator for safekeeping when this request is issued before the announcement of a formal examination.

15.10 Mobiles must be switched off during lessons and mocks and not be left on the tables or desks or handed in for safekeeping.

15.11 College community members cannot communicate through personal emails or social media channels inside or outside the college. Communication is acceptable via official SMS and email systems only.

15.12 If the Principal has reasonable grounds to suspect inappropriate communication between staff and students, then mobiles or other devices may be secured for examination.

16. Training

16.1 As part of their induction, All new staff members will receive training on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation.

16.2 All staff members 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 meetings).

16.3 The Director of Studies (Pastoral) 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 update their knowledge and skills about online safety regularly, at least annually.

16.4 The Principal will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

16.5 Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our Child Protection and Safeguarding policy and the Prevent policy.

17. Remote Learning:

17.1 Where there are periods in which the college is forced to close yet continue to provide education (such as during the COVID-19 Pandemic), it is essential that Westminster Tutors supports staff, students, and parents to access learning safely, especially considering the safety of our vulnerable students.

17.2 Staff and volunteers are aware that this challenging time potentially puts all children at greater risk, and the college recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk.

17.3 Staff and volunteers will continue to be alert to any signs of abuse or effects on learners' mental health that are also safeguarding concerns and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy, and where appropriate, referrals should still be made to children's social care and as required, the police.

17.4 Online teaching should follow the same principles in the college's staff and students' code of conduct. Additionally, the college name will ensure that any use of online learning tools and systems aligns with privacy and data protection/GDPR requirements.

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 they may have. Advice will also be issued on which staff 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 for ensuring the safety (including online safety) of college community members, with the day-to-day responsibility being delegated to the Director of Studies (Pastoral). The Principal and the Director of Studies (Pastoral) are aware of the procedures to be followed in the event of a severe online safety allegation being made against a member of staff, which is in line with our main safeguarding reporting procedures.

17.7 Staff working remotely should, wherever possible, use their college-issued IT equipment.

However, they may use their computer equipment if it is not practical and follows the college's Data Protection Policy. Staff are responsible for the security of personal data and 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 Director of Studies (Pastoral) logs behaviour and safeguarding issues related to online safety.

19. Links with other Policies and Procedures

- Child Protection and Safeguarding policy.
- Prevent policy.
- Behaviour policy.
- Staff disciplinary procedures.
- Data Protection Policy and Privacy notices.
- Complaints Procedure.

20. Liability of the College

20.1 Unless specifically negligent under the terms of this policy, the college does not accept any responsibility to the parents or students for a problem caused by a student's use of mobile phones, email, or the Internet while at the college.

21. Monitoring and Review:

21.1 These arrangements are subject to continuous monitoring, refinement, and audit by the Principal, who will undertake a complete annual review, including its implementation and the efficiency with which the related duties have been implemented. This review will be undertaken in a Governance Advisory Board meeting.

21.2 Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements, which will be made available in writing or electronically.

Updated by S Doherty, Summer 2023
Date of Next Review: Summer 2024