Westminster Tutors

Acceptable Use & Digital Safety Policy

2024-2025

Contents

1. Introduction

1.1 Using technology as a tool has become integral to college and home life.

1.2 Westminster Tutors is committed to the practical and purposeful use of technology for teaching, learning, and administration. It is also committed to protecting its staff, students, parents, and visitors from the illegal or harmful use of technology by individuals or groups, knowingly or unknowingly.

1.3 The college actively promotes parent participation in safeguarding the welfare of students and promoting the safe use of technology.

1.4 This policy applies to the use of:

- All technology devices and equipment connected to the college network;
- All technology devices supplied by the college to employees and contractors, both onsite and offsite;
- All applications and IT services provided by the college for teaching, learning and administration; and
- All applications and IT services are accessible online via the college network or a technology device.

1.5 Staff, students, parents, and visitors can request a copy of this policy, which is also available on the college website.

1.6 Failure to read this policy and its requirements will not be accepted as a defence/excuse in case of a breach of this policy and its requirements.

2. Purpose

2.1 Promote responsible use and care of technology and IT services available to staff, students, parents and visitors.

2.2 Outline the acceptable and unacceptable use of technology and IT services at the college, both on and offsite.

2.3 Outline the roles and responsibilities of all staff, students, parents and visitors.

2.4 Educate and encourage students to make good use of the educational opportunities presented by access to technology at the college.

2.5 Safeguard and promote the welfare of students, in particular by anticipating and preventing the risks arising from:

- Exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials).
- Inappropriate contact from staff.
- Inappropriate contact with strangers.
- Cyberbullying and abuse.
- Copying and sharing personal data and images, etc.

2.6 Outline digital filtering and monitoring on college devices and the college network.

2.7 Outline requirements for reporting misuse of technology.

3. Scope

3.1 This policy applies to all staff, students, parents and visitors.

3.2 The college will take a broad and purposive approach to consider what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware, software and services, and applications associated with them, including:

- The college network, WiFi and internet access.
- Tablets, desktops, laptops, and thin client devices.
- Mobile phones, smartphones, smart watches and other smart wearables.
- Digital devices for audio, still images and moving images (e.g. personal music players and GoPro devices);
- Digital displays.
- Communication and collaboration applications (e.g. email and Google).
- Virtual Learning Environments (e.g. Google Classroom).
- Mobile messaging apps (e.g. Snapchat and WhatsApp).
- Social media (e.g. Facebook, Instagram, TikTok), etc.

3.3 This policy applies to using technology on and off college premises.

3.4 This policy applies to any college community member whose actions threaten the college's culture or reputation.

3.5 This policy applies to any college community member where staff, students, parents or visitors are put at risk.

4. Roles and Responsibilities

4.1 This policy document is the responsibility of the college Principal.

4.2 The Principal is responsible for publishing this policy and the ongoing implementation and monitoring.

4.3 The Principal is responsible for ensuring that technology and IT Services are deployed and monitored per this policy.

4.4 All staff, students, parents and visitors are responsible for adhering to the policy.

5. Safe Use of Technology

5.1 The college is committed to the safe and purposeful use of technology for teaching, learning and administration.

5.2 The use of technology should be safe, responsible, respectful to others, and legal. Staff, students, parents, and visitors are responsible for their actions, conduct, and behaviour when using technology at all times.

5.3 The college will support the use of technology and make internet access as unrestricted as necessary whilst balancing the educational needs of our students, the safety and welfare of staff, students, parents, and visitors, and the security and integrity of our systems.

5.4 Monitoring, logging and alerting tools are in place to maintain technology safety, safeguarding and security for the protection of Staff, Students, Parents and Visitors.

5.5 We want students to enjoy using technology and to become skilled users. Technology has become a fundamental part of education, not only as a vehicle for delivering great teaching and learning but also as a platform for collaboration and productivity.

5.6 Students will be educated about the importance of safe and responsible technology use to help them protect themselves and others online.

5.7 The college actively encourages parents' participation in helping promote the safe use of technology with their children.

5.8 Any concern regarding unsafe or inappropriate use of technology should be reported to a teacher, the DDSL or the Principal as soon as possible. The Principal will report any serious incident involving unsafe or inappropriate technology to the Chair of the Governance Advisory Board.

5.9 All users of technology may find the following resources helpful in keeping themselves safe online:

- UK Safer Internet Centre
- Internet Matters - resources
- Google Family Safety
- Common Sense Media

6. The Right to Use College Network and Equipment

6.1 School employees and students will be allocated a username and password for accessing technology devices and services.

6.2 Some shared resources will have a generic username and password for access.

6.3 All college technology remains the property of the college. The college may reasonably request the device or withdraw access to the service at any time, and if applicable, the device must be returned to the college.

6.4 Only college devices should be connected to the college network, and personal devices should only be connected to the wtguest network.

6.5 Any attempt to access or use any user account or email address for which a staff member, student, parent or visitor is not authorised is prohibited.

6.6 Designated devices may be issued to college employees and students for teaching, learning and administration:

- School employees and students are responsible for the safety and security of a designated device when taken out of college.
- School-issued devices and associated peripherals should be returned in good condition (excluding ordinary wear and tear) and in working order.
- School-issued devices are insured against accidental damage, loss and theft; the assignee is liable to pay the Westminster Tutors insurance excess.

6.7 Resource devices are available in the college for employees and students to use in general work, lessons, and specialist applications.

6.8 School employees and students may not use, or attempt to use, IT resources allocated to another person except when explicitly authorised.

6.9 For security purposes, users must log off or lock their computer at all times when they step away from it and must log off and shut down their device at the end of the day.

7. Appropriate Use of Technology for Digital Safety

7.1 The college provides system and application accounts for staff, students, parents, and guests when required.

You must:

- Not allow other people to use your account.
- Do not use someone else's account.
- Lock your device or log out of your account when not in use.

- Only use college applications and email for official college business and digital correspondence.
- Not send messages or emails from college accounts that purport to come from someone other than the person sending the message.

Staff and students must:

- Use official college accounts on approved collaborative platforms

7.2 The college provides technology hardware and software to support education and the running of the college business.

- Users of college technology equipment are expected to take care of the equipment through responsible behaviour.
- School technology should not be removed from the college site except where:
  - The device is assigned to an individual member of staff.
  - There is written permission from the Principal.
- School technology assigned to staff and students is the assignee's responsibility.
- You should not leave portable technology equipment, including college-issued devices, unattended.
- Loss or damage of college technology should be reported to a teacher or member of the School Leadership Team at the earliest opportunity.
- Theft of college technology assigned to an individual member of staff or to a student should be reported to the police and to a teacher, member of the School Leadership Team, or at the earliest opportunity, along with a crime reference.
- Deliberate abuse or damage of college equipment will result in the culprit(s) being billed for the total replacement costs.
- Do not:
  - Attempt to install software onto a college-owned or college-issued device.
  - Download or access illegal software on college devices.
  - Download any software packages from the college network onto portable media or personal devices.
  - Attempt to copy or remove software from a college-owned or college-issued device.
  - Attempt to alter the configuration of the hardware equipment or any accompanying software unless under the written instruction of the college.

7.3 The college provides technology resources for accessing and storing Data.

Do not:

- Access or attempt to access data for which you are not authorised.
- Interfere with digital work belonging to other users.
- Share private, sensitive or confidential information unless you have the auth
  - You have the authority to share
  - The method of sharing is secure
- It is the responsibility of technology users when accessing data to be aware of Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights.

7.4 The college endeavours to safeguard and, where possible, mitigate all technology security risks.

7.5 The college has filtering systems to block access to unsuitable material wherever possible and protect the welfare and safety of staff, students, parents and guests.

You must not:

- Try bypassing college filtering systems whilst using college devices or the college network.
- Use software or network routing to bypass filters and access blocked sites.
- Try bypassing technology security systems whilst using college devices or the college network.
- Use software or network routing designed to bypass college technology security systems.
- Access to unsuitable material on a college device or the college network should be reported to a teacher, or a member of the School Leadership Team at the earliest opportunity.
- The college has technology security systems to block and protect against computer viruses or malicious software such as spyware.
- Concerns regarding viruses and other malicious software should be reported to a teacher, member of the School Leadership Team or IT Support Team at the earliest opportunity.

7.6 All technology users must ensure their welfare and that of others on personal and college devices.

- Cyberbullying - Students must not use their or the college's technology to bully others.
- Strangers - Students must not use their own or the college's technology to contact or engage with people they do not know.
- Sexting - Students must not use their own or the college's technology to create or share sexualised content, including images, audio, video and text.

7.7 Concerns regarding welfare associated with the use of technology should be reported to a teacher, member of the School Leadership Team, or Designated Safeguarding Lead as soon as possible.

7.8 The college provides appropriate access to the Internet to support education and running the college business.

- The internet provides technology users unprecedented opportunities to obtain information, engage in discussion, and liaise with individuals, organisations and groups worldwide to increase skills, knowledge and abilities.
- The college actively supports access to the widest variety of available information resources, accompanied by developing the skills necessary to filter, analyse, interpret and evaluate information encountered.
- Staff, students, parents and visitors must not use a college device or the college network to intentionally visit internet sites that contain obscene, illegal, hateful, abusive, offensive, pornographic, extremist or otherwise inappropriate materials.
- Staff, students, parents and visitors must not use a college device or the college network to access gambling websites.

- Staff, students, parents and visitors shall be responsible for notifying a member of the School Leadership Team or the Deputy or Designated Safeguarding Lead of any inappropriate material accessed on a college device or the college network so that access can be blocked.
- The privacy of staff, students, parents, and visitors must always be recognised and respected on social media sites.
- Staff should not connect with any currently enrolled students on social networking sites or via personal mobile phones.
- Staff, students, parents and visitors of the college must not make offensive or inappropriate comments, including bringing the college's name and reputation into disrepute on any forum/platform, such as social media sites (whether using a college device or not) where a connection between the user and the college can reasonably be made.

8. Allocated devices: access & privacy

8.1 Access to assigned devices and IT content:

- School technology devices assigned to staff and students are for the sole use of the assignee.
- Westminster Tutors' devices may be loaded with remote support applications, which enable IT support staff to log on to the devices and provide remote assistance with or without the assignees' permission.
- Westminster Tutors reserves the right to access an assigned device and monitor its use and content under the following exceptional circumstances, including but not limited to:
  - To detect and prevent crime.
  - To enable system security protection (e.g. Virus, Malware, Hacking or other Risk).
  - To investigate potential misuse, abuse and illegal activity.
  - To monitor compliance with employment and statutory obligations.
  - To guarantee the integrity of the college devices, technology and IT systems.

9. Photographs and images

9.1 The college abides by data protection legislation, namely, the General Data Protection Regulation 2018 (as amended, extended or re-enacted from time to time), and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and internal purposes, such as a yearbook or on a parent portal. Parents and guardians may withdraw this permission anytime by informing the college's Administration Team in writing.

9.2 Staff, students, parents and visitors are not permitted to use devices such as mobile phones, cameras, smart watches or digital recorders to photograph or record members of staff or students without their permission. Safe and appropriate use of recording equipment must be discussed with the students as part of the curriculum and referred to whenever recording occurs. Permission may be granted by the college in the event of performances/events organised by the college.

9.3 Parents are asked to be considerate when taking videos or photographs at college events and are requested not to publish material of other children in any public forum without the permission of the relevant family. It is illegal to sell or distribute recordings from events without permission. Any parent who does not wish their student to be videoed or photographed at college events by other attendees must notify the college in advance and in writing.

10. Use the School equipment for personal use

10.1 Personal devices must not be connected to the college network other than the wtguest WiFi network.

11. Procedures for Reporting

11.1 Staff, students, parents, and visitors of the college with a concern or an incident regarding technology should take the following actions:

- Stop the problem or remove the technology.
- Prevent exposure of the incident to others.
- Record the nature of the incident and those involved.
- Preserve evidence to enable investigation if required.
- Report the incident or concern to a teacher, college Head, Designated Safeguarding Lead or IT Support Team as appropriate.
- Staff must not carry out any investigations unless authorised by the Principal.

11.2 Any concern regarding unsafe or inappropriate use of technology or welfare associated with the use of technology should be reported to a teacher, college Head or Designated Safeguarding Lead as soon as possible.

11.3 Access to unsuitable material and concerns regarding viruses and other malicious software on a college device or the college network should be reported to a teacher or a member of the School Leadership Team as soon as possible.

11.4 Loss, damage, or theft of college technology should be reported to a School Leadership Team member as soon as possible; theft should also be reported to the police, and a crime reference should be obtained.

11.5 Students must take responsibility for using IT equipment at college and home; should parents or guardians have concerns or become aware of an issue, we strongly encourage prompt communication with the college to offer advice and support.

11.6 The college must report severe concerns to Local Authority Safeguarding Teams or the Police, following statutory requirements.

12. Removal of network rights/sanctions

12.1 Anyone found abusing the Acceptable Use & Digital Safety Policy on the use of computers may have their network rights removed and may be subject to further disciplinary action.

12.2 The college reserves the right to remove network access at any time.

12.3 The college may inform the police or other law enforcement agencies of any use that could give rise to criminal proceedings.

12.4 The college takes its responsibilities regarding digital safety and the use of technology by staff, students, parents, and visitors seriously and understands the importance of monitoring, evaluating, and reviewing its policies and procedures regularly.

Ownership and consultation	
Document author (name)	Sean Doherty, Principal

Audience	
Audience	Principal, college staff, students, and parents

Version control	
Implementation date	September 2024
Review date	September 2026