The Westminster
Specialist College

2022/2023

E-Safety and Acceptable Use of ICT Policy

Approved by Board of Governors on:	15/12/2022
Signed by Chair of Governors:	P Coldicott
Head of College:	O Flowers
Lead Personnel:	O Flowers
Date of Review:	15/12/2024

Rationale

It is the duty of the College to ensure that every student in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world.

This policy, supported by the Acceptable Use Policies (AUP; see appendices) for staff, governors, visitors and students, is to protect the interests and safety of the whole College community and aims to provide clear advice and guidance. This policy is about empowering adults at the college to identify the risks associated with the digital world and how to manage the risks safely and effectively. It is linked to the Health and Safety Policy.

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet, technologies provided by the College (such as PCs, laptops, whiteboards, tablet, voting systems, digital video and camera equipment, etc) and technologies owned by students or staff.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of students and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in College and, more importantly in many cases, used outside of College by students include:

- The Internet
- e-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as Smart Phone and Tablets.

Whole College approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this College:

1. An effective range of technological tools which are filtered and monitored which support adults to make appropriate choices.
2. Policies and procedures, with clear roles and responsibilities;
3. A comprehensive e-Safety education programme for students and staff.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this College and the Head of College, with the support of governors, aims to embed safe practices into the culture of the College. The Head of College ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

The responsibility for e-Safety has been designated to a member of the College senior leadership team and e-Safety Co-ordinators have been identified.

Our e-Safety Coordinators ensures they keep up to date with e-Safety issues and guidance through liaison with Broadband Sandwell's e-Safety Officer and through organisations such as The Student Exploitation and Online Protection (CEOP) and 360 degree safe. The College's e-Safety Coordinators ensures the Head of College, Senior Leaderships Team and Governors are updated as necessary.

Staff awareness

- All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.
- New staff receive information on the College's AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of students within the context of e-safety and know what to do in the event of misuse of technology by any member of the College community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-safety records of concern are completed by staff as soon as incidents occur and are reported directly to the College's designated safeguarding team, Mrs Joanne Turner, Miss Gemma Webb, Mr Oliver Flowers and Mrs Denise Taylor.

All staff working with students are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following College e-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in College.

Internet:

- The Westminster Specialist College will use TrustNet "filtered" Internet Service, which will minimise the chances of students encountering undesirable material.
- Staff, students and visitors have access to the internet through the College's fixed and mobile internet technology.
- Staff should email College-related information using their Openhive/@twspecialistcollege.co.uk address and not personal accounts.
- Staff will preview any websites before recommending to students.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- If staff or students discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety coordinator(s) detailing the device and username. Agilisys can then be informed and contact to TrustNet can be instigated.
- Staff and students are aware that College based email and internet activity is monitored and can be explored further if required.

- Students using the World Wide Web are expected not to deliberately seek out offensive materials. Should any students encounter any such material accidentally, they are expected to report it immediately to a teacher and then Agilisys so that the Service Provider can block further access to the site.
- Students are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.
- They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved College project.
- Students consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the College's behaviour policy.
- A summary of these ICT rules are displayed in the ICT suite and all areas with ICT resources. Students will be asked to sign to this agreement, ensuring that they are aware of expectations. (See Appendix). Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.
- The internet user agreement also appears when students log in to networked computers in College. They are required to click to agree to the policy before they are allowed to use the computers.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other students or staff.

Mobile technology (laptops, iPads etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Staff should only use the laptop which is allocated to them.
- Mobile technology for student use, such as iPads and laptops are stored in a locked cupboard. Access is available via the College office keyholders or Agilisys. Members of College staff should sign in/out the technologies before and after each use.
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff or students are to be used during lessons at College. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent. If students bring in mobile phones (for the purpose of safety if they travel to and from College alone), they should be kept switched off and out of sight all day, and will remain the responsibility of the student in case of loss or damage. Any students not following these rules will be dealt with using the College's behaviour policy.

Data storage

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one or to the Google Drive Account.

- The College discourages the use of removable media however if they are used we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside College or sent by post or courier.
- Staff laptops should be encrypted if any data or passwords are stored on them.
- IEPs, assessment records, student medical information and any other data related to students or staff should not be stored on personal memory sticks but stored on an encrypted USB memory stick provided by College or on our secure SharePoint platform.
- All staff are required to sign a personal data encryption agreement before being issued with an encrypted memory stick. (See appendix).
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the College Senior Leadership Team.

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should College students or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in College requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the College, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the College and Local Authority Disciplinary Policy applies.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- place a student or young person at risk of harm;
- bring the College into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting images that are discriminatory or offensive or links to such content.

The College reserves the right to monitor staff internet usage. The College considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

Digital images

- Use only digital cameras and video cameras provided by the College and under no circumstances use personal equipment such as digital cameras or camera phones to store images of students.

- Ensure you are aware of the students whose parents/guardians have **not** given permission for their student's image to be used in College. An up to date list is kept in the College administrative office.
- When using students' images for any College activity, they should not be identified by their name.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Providing a comprehensive E-safety education to students and parents

- All staff working with students must share a collective responsibility to provide e-safety education to students and to promote e-safety in their own actions.
- Formally, an e-safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Even if e-safety is not relevant to the area of ICT being taught, it is important to have this as a 'constant' in the ICT curriculum.
- Informally, a talking culture is encouraged in classrooms which allows e-safety issues to be addressed as and when they arise.
- E-Safety themes are also woven into the fabric of the College curriculum through SHaLT.
- Staff will ensure students know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the ICT Coordinator with responsibility for E-safety.
- When students use College computers, staff should make sure students are fully aware of the agreement they are making to follow the College's ICT guidelines.
- Students will have the opportunity to educate parents through a range of activities.

Maintaining the security of the College IT Network

Agilisys maintains the security of the College network and is responsible for ensuring that virus protection is up to date at all times. However, it is also the responsibility of the IT users to uphold the security and integrity of the network.

Virtual Learning Gateway (VLE)

Staff and students have access to the SharePoint, provided and maintained by Agilisys.

Students/staff details or sensitive, confidential information will be stored on here and all login credentials including passwords must not be written down.

All classes may provide work for publication on SharePoint and digital images and work can be stored. Subject staff will be responsible for ensuring that the content of the students' work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status.

Complaints procedure

As with other areas of College, if a member of staff, a student or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the e-safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern will be recorded using a Record of Concern

proforma and reported to the College's designated safeguarding officer in accordance with College's student protection policy. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Monitoring

The Head of College or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the College at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain College business related information; to confirm or investigate compliance with College policies, standards and procedures, to ensure the effective operation of College ICT, for quality control or training purposes, to comply with a Subject Access Request under the GDPR, or to prevent or detect crime.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the College Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the College's Designated Safeguarding Team either Joanne Turner, Denise Taylor, Gemma Webb or Oliver Flowers.

The Westminster College
ICT Acceptable use policy for students for use at home (H) and at College (S).

The College has installed computers and Internet access to help our learning. These rules will keep us safe and help us to be fair to others.

- I will utilise the technology for learning during designated lesson times. However technology can also be utilised for leisure time at and appropriate time and in an appropriate way (S/H).
- I will only use my login and password and never share these with others. (S) (H)
- I will ask permission before bringing in memory sticks as I understand challenges with virus protection (S)
- I will only open and delete my own files. (S)
- The messages I send will be polite, sensible and follow traditional forms of electronic etiquette. (S) (H)
- I will never give out my own or other people's name, address or phone number online unless for the purposes of work. (S) (H)
- I am permitted to upload images of College activities to social networking site but only if I have the express permission from those in the pictures or responsible for the content. (S) (H)
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. (S) (H)
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away. (S) (H)
- I understand that the College can check my computer use in order to support me to keep safe when using electronic devices.
- I will work with the College personnel on e-Safety so I can keep myself safe whilst online. (S)

Student Signed: _____ Date:_____

Parent Signed: _____ Date:_____

The Westminster College
ICT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from e-safety incidents and promote a safe e-learning environment for students.

- I will only use the College's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in College.
- I will not disclose my password to anybody else.
- When accessing College email, SharePoint or any other sensitive information relating to The Westminster College, employees will ensure that it is conducted on a device that had the appropriate security measures (anti-virus, firewall, encryption) and that locked out when away from the device and logged off each of the sites after use.
- I will ensure that any online communications with staff, parents and students are compatible with my professional role.
- I will not give out my own personal details to students or parents.
- I will send College business emails using my College email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of students will only be taken and used for professional purposes in line with College policy with consent of the parent or carer. Images will not be distributed outside of College without the permission of the parent/carer and Head of College.
- If it is necessary to bring my own personal devices into College, these will only be used during non-contact time without students.
- **I will report any e-safety concerns to the designated safeguarding officer immediately using the E-safety Record of Concern.**
- **Mobile phones will be out of sight and switched to silent.**
- **I will ensure that my online activity, both in College and outside College, will not bring my professional role into disrepute.**
- **I will support the College's e-safety policy and help students to be safe and responsible in their use of ICT and related technologies.**

I understand the procedures and agree to follow them with immediate effect.

Print Name: _____

Signed: _____ Date: _____

The Westminster College
Data Security

Following a review of procedures in place to store sensitive data in line with National recommendations the following practice is to be adhered to:-

> ***Sensitive data consists of any information which is personal to individuals or deemed sensitive or valuable to the College.***

Staff should only save sensitive data in the following secure formats:-

1. On the learning platform (SharePoint)
2. On the encrypted USB memory stick provided
3. On the encrypted laptop provided
4. Onto the Google Drive account provided as part of your employment (@westminstercloud.co.uk)

This ensures that no legal action can be taken for lost data.

Staff are encouraged to hold all of their data on their College laptop that has a built-in level of encryption. If this is not possible and they have not been allocated a laptop they are encouraged to save all of the data onto their Google Drive account provided as part of their employment. The password for this account should not be written down anywhere and the Google Drive Account should be logged out or lock when not in use.

If you lose your encrypted memory stick or are unable to open it because of a password error, you must inform the Deputy Head of College(s) or Head of College without delay. It is imperative that you do not share or write down your password. You may add a question prompt reminder when first accessing your memory stick, which can be used if you have forgotten your password. It is your responsibility to keep the data from your memory stick regularly backed up in another secure format as detailed above. Sensitive data should not be sent via email to external agencies, third party agencies or those no employed by the College unless it is encrypted/password protected.

Failure to follow these guidelines will be treated seriously and could lead to disciplinary procedure.

I understand the procedures and agree to follow them with immediate effect.

Name _____ Signed_____

Date _____

E-Safety Record of Concern

<table>
<tr><td>Name of Student</td><td colspan="3"></td></tr>
<tr><td>DOB</td><td colspan="3"></td></tr>
<tr><td>Date of incident/disclosure</td><td></td><td>Time</td><td></td></tr>
<tr><td>Names of any other Staff/Students Present</td><td colspan="3"></td></tr>
<tr><td rowspan="2">Record any disclosure from the student using their words. Use:
• Tell
• Explain
• Describe
• Outline

To clarify/gather information
USE NO FURTHER QUESTIONS.</td><td colspan="2">Who?</td><td>What?</td></tr>
<tr><td colspan="2">Where?</td><td>When?</td></tr>
<tr><td>Why are you concerned about the student?</td><td colspan="3"></td></tr>
<tr><td>Detail anything you have observed and when.</td><td colspan="3"></td></tr>
<tr><td>Detail any websites/games/films the student discussed with you. Please include Avatar names, online friends names where known.</td><td colspan="3"></td></tr>
</table>

What catergory does the disclosure best fit with?	Grooming		
	Cyberbullying		
	Misuse of Social Networking site		
	Sexting		
	Gaming		
	Underage Films		
	Misuse of Digital Camera		
	Other (please specify)		
Detail anything you have heard and when.			
Detail anything you have been told, by who and when.			
Name (Print)		Date	
Position:		Signature	

E-Safety Record of Action

Name of e-Safety Coordinator/DSL record of concern handed to:	
Date:	
Action(s) to be taken:	
Outcomes of action:	
Name (print):	Date:
Designation:	Signature: