Central Academy
The best in everyone™
Part of United Learning

Acceptable Use of Technology Policy Guidance for Students March 2024

www.rrca.org.uk

DOCUMENT CONTROL

Author/Contact	Mark Wood	
Version	05	
Status	Approved	
Publication Date	June 2017	
Review Date	Annually	
Approved/Ratified by:	Local Governing Body	Date: March 2024
Distribution: Central Academy staff PLEASE NOTE, this version of the document contained within the Policy Folder on the 'V' drive in the Policy Folder is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.		

Version	Date	Comments	Author
02	June 2017	Reviewed and Updated	M Wood
03	Oct 2019	Reviewed – no changes	M Wood
04	May 2022	Reviewed – no changes	M Wood
05	March 2024	Reviewed – changes to some out of date language	M Wood

Acceptable Usage of Technology - Guidance for Students

School Computers (desktops, laptops and chromebooks)

1) Do not install, attempt to install or store programs of any type on the computers without permission.
2) Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources. Report any such damage to a member of staff.
3) Do not use the computers for commercial purposes (e.g. buying or selling goods).
4) Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs, iPods, MP3 players etc.) unless you have the permission of the member of staff responsible for ICT.
5) Do not eat or drink near computer equipment.
6) Respect, and do not attempt to bypass security in place on the computers or attempt to alter the settings.
7) Do not leave your computer logged on whist unattended.
8) The use of personal computing devices is bound by the school's *Mobile Device* policy.

Internet (school owned and personal devices)

1) Do not access the Internet unless for study or for school authorised/supervised activities.
2) Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, abusive, or hurtful to others, or which may bring the school into disrepute. If you come across anything like this, report it to a member of staff.
3) Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
4) Do not assume that information you find on the internet is trustworthy. Some sources of information may be published to deliberately mislead.
5) Do not engage in 'chat' or social networking activities over the Internet unless these are as part of a lesson and under supervision of your teacher.
6) Never arrange to meet anyone unless accompanied by a parent, guardian. People that you meet online are not always who they appear to be.

Security and Privacy (school owned and personal devices)

1) Do not disclose your password to others, or use passwords intended for the use of others.
2) Do not access, copy, remove, or otherwise alter the files of without their express knowledge and permission.
3) Never provide personal information about yourself, such as your DOB, home address, telephone number or school name, or send photographs of yourself or others, unless you are given permission by a member of staff to do so. This could be in a social media setting, in an online profile or online conversation.
4) Do not use computers or mobile devices in a way that harasses, harms, offends or insults others.
5) Your school Office 365 account and other services you access through this account are not private, and staff may review files and communications to ensure that users are using the system responsibly.

Email (school computers and mobile devices)

1) Be polite and appreciate that other users might have different views. The use of strong language, swearing or aggressive behaviour is not allowed.
2) Never open attachments to emails unless they come from someone that you know and trust, and you are expecting the communication. Similarly, never click on links in emails

before checking they are legitimate. QR codes can point to malicious websites – always check the internet address before opening it.

3) The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, extremist, sexual or other inappropriate content.

Photographs and Video

1) Do not take pictures or record film of any students or members of staff, while in school or on school trips, without the permission of those being photographed or filmed.
2) If you need to photograph or film other students as part of an educational activity (e.g. drama rehearsal), you should use a school camera and you must seek permission from a teacher to make the film and check that students involved give their consent.
3) Where personal devices are used, such as on school trips with general permission from the trip leader, consideration should be given to the appropriateness of uploading pictures or film to social media and if requested by the subject of the images, remove them from social media platforms. Uploading inappropriate photos or videos could result in disciplinary action.
4) Never send, print, display or otherwise transmit images which are unlawful, obscene, abusive, or hurtful to others, or which may bring the school into disrepute. This includes ‘sexting’ - the generating and/or sharing of text, images, or video of a sexual/indecent nature via a mobile phone, handheld device or website involving myself and/or others.

Acceptable Usage of Technology Policy Agreement – Students

1) You must read and sign this agreement before you can be allowed to use the school's ICT resources.
2) You must agree to the school viewing on your school account, with just reason and without notice, any e-mails you send or receive, material you store on the school's computers, or logs of websites you have visited.
3) You must only access those services you have been given permission to use.
4) Personal storage devices such as USB 'memory sticks' may be brought into the Academy but only to assist with your school work.
5) You must adhere to all instructions set out in the attached Guidance Document.
6) You must also abide by the school's *Mobile Devices* policy.
7) If you become aware of a breach of this policy it is your responsibility to report it to a member of staff.

Penalties for misuse of computer systems will depend on the nature and seriousness of the offence. Disciplinary action may be taken against students who contravene this policy. The school, for various legitimate business practices, may need to monitor the use of e-mail and internet access from time to time for the following reasons:

- to establish the existence of facts (e.g. the details of an agreement made)
- to monitor for quality control and staff training purposes
- to prevent or detect crime
- to investigate or detect unauthorised use of the school's telecommunication system (including e-mail and internet)
- to intercept for operational purpose such as protecting against viruses and making routine interruptions such as forwarding e-mail to correct distributions
- to gain access to routine business communications (e.g. checking e-mail) when students are on holiday or sick leave

---

I confirm that I have read the Acceptable Usage of ICT - Guidance for Students, understand it and intend to comply with its obligations.

Full name (print) ……..

Signature ……..

Date ……..