Staff & Guests Acceptable Use Agreement

At Venture Multi Academy Trust we value the diversity of backgrounds of all pupils, families and wider school communities.

We promote the fundamental British values of; democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs.

Our schools reflect British values in all that we do. We aim to nurture our children on their journey through life so they can grow into safe, caring, democratic, responsible and tolerant adults who make a positive difference to British society and to the world. We encourage our children to be creative, unique, open-minded and independent individuals, respectful of themselves and of others in our schools, our local communities and the wider world.

Venture Multi Academy Trust provides ICT equipment for use by staff, students and volunteers. They offer access to a vast amount of information for use in studies, offering great potential to support the curriculum.

The ICT equipment is provided and maintained for the benefit of all staff and students, who are encouraged to use and enjoy these resources, and ensure they remain available to all.

Where the term "staff" is used in this document, please note that these statements also apply to guests (e.g. volunteers and visitors.)
The following guidelines must be adhered to:

Equipment

- Do not install, attempt to install, or store programs of any type on the ICT equipment without permission.
- Do not damage, disable, or otherwise harm the operation of ICT equipment, or intentionally waste resources.
- Do not use the ICT equipment for commercial purposes, e.g. buying or selling goods for personal use. Trading on-line for the benefit of the school is permitted, (under compliance with the school's standard Purchase Order procedure).
- Do not use external storage devices (such as flash drives, external hard drives etc.) An encrypted flash drive can be provided if required.
- Always check mobile equipment (e.g. laptops, tablet PCs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Do not eat or drink near ICT equipment.
- Do not connect any personal devices to the network, if this is required for work purposes permission must be gained from the Head of School and then the Network Manager.
- Wearables, such Smart Watches are included in the Mobile Phone Policy. Some devices are capable of taking photos. Personal photographic devices are not to be used in school.
- Always report any lost, damaged or faulty equipment immediately to the network manager or ICT TA.
- All staff devices must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

- **Mobile Equipment**
    - Mobile equipment such as laptops, iPads and cameras may be loaned to staff in order for them to complete their work. These devices are for the express use of the member of staff and not for use by anyone else in their household. They remain the property of the school despite lengthy loan periods.
    - In order to comply with the school's insurance policies, mobile equipment must not be left unattended. This includes but is not limited to being left in parked cars and public places or transport such as cafes and trains. Loss due to lack of care may result in the member of staff being charged for replacement.
    - ICT equipment left unattended in school must be locked away appropriately, either in class cupboards or lockable charge trollies.
    - Any loss of ICT equipment must be reported to the Network Manager immediately, as there may be ramifications according to GDPR (2018).
    - At the end of the loan period all equipment will be checked and repair costs associated with unreported damage may be charged to the member of staff.

Reviewed by Mr D. Harvey and Mrs S. Tully on 17/12/2018

Security & Privacy

- It is your responsibility to ensure you have read and understood the school's Password and Security policy and conform to the policy statements within it.
- Do not post, confidential or sensitive information on the Internet unless on approved websites for school business and only then with permission from the Head of School.
- Do not use the computers in a way that harasses, harms, offends or insults others.
- Respect, and do not attempt to bypass, security in place on ICT equipment, or attempt to alter the settings.
- Network administrators have full access and will review files and communications to ensure that users are using the system responsibly.
- Any information obtained from the Network or school websites and software, e.g. Sims regarding pupils, staff, parents or other associated bodies is strictly confidential and disclosure of such information to another person is a serious breach of GDPR.
- ICT equipment should never be left unattended whilst logged in unless locked.
- No school data should be stored on personal devices as these will not be encrypted and this will be a breach of GDPR.
- Do not take or distribute images of anyone without their permission.
- Remember to regularly check photo permissions of children before posting on school websites/social media accounts.

Internet

- You should access the Internet in school, only for school activities via the school network.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as students or staff. This includes abiding by copyright laws.
- Do not engage in "chat" activities over the Internet, via the school network. This takes up valuable resources which could be used by others to benefit their studies.
- A filtering system is in place for Internet access but it is impossible to guarantee that all inappropriate websites are filtered. Users must not attempt to find such material. It is the user's responsibility to report the address of any such material accidentally encountered so that it can be filtered.
- Staff are reminded that accessing websites which contain violent, racist or inappropriate content may impact on their professional role in school and bring the school into disrepute.
- Social Networking Websites, (e.g. Facebook and Twitter) may be accessible in school for the use of school accounts. We understand that staff may use these sites for their own personal communication. As a school we would like to remind employees that they must abide by the terms set out in the Social Networking Policy and not log into personal accounts on school devices.

Email & Messaging

- School email addresses are provided for staff solely for the purpose of school business and must not be used for personal messaging.
- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed,
- Never open messages, attachments of follow hyperlinks unless they come from someone or an organisation you already know and trust. They could contain viruses or other potentially unwanted programs such as adware and malware.
- The sending or receiving of a message containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of ICT staff.
- Do not send sensitive or confidential data via email, unless appropriately encrypted.
- Do not use children's full names in emails/ messages, only use initials where identification is necessary.
- Do not send or forward "chain" mails, petitions, jokes etc. This takes up valuable resources and other people may not appreciate them. They could be interpreted as offensive.

Failure to conform to this agreement can result in disciplinary procedures.