

Magnus Church of England Academy

Student ICT Acceptable Use and Responsibility Policy

The academy has provided computers for use by students, offering access to a vast amount of information and software for use in studies, offering great potential to support the curriculum.

Academy computers are provided and maintained for the benefit of all students, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. As a student in the academy, you are responsible for using the computer systems in a safe and appropriate manner both online and offline just as you are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn and/or disciplinary action will be taken.

Equipment

- Students should not attempt to install or download software of any type onto the computers.
- Students should not attempt to download files of any types without prior permission or instruction for a member of staff.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Inappropriately altering the computer display equipment in any way. (altering brightness/colour, changing display language etc.)
- Tampering with connected peripheral/attached components to the computer system i.e. (monitor, mouse, keyboard) by unplugging/plugging into the computer system without supervision or permission.
- Use of computers within the academy are for educational purposes only. Activities such as playing games, checking social media accounts, listening to music and watching videos are inappropriate, unless part of your lesson.
- Files brought in on removable media (such as floppy disks, CDs, flash drives etc.) should be checked with antivirus software.
- Files downloaded from emails should be checked with antivirus software.
- Mobile equipment (e.g. laptops, tablets, smartphones etc) should not be connected to the school network without permission of the ICT department.
- No eating or drinking within computer rooms or near computing equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's log on, name or password.
- Use of another student's login information or account for any purposes is strictly prohibited.

- Always get permission before revealing your home address, telephone number, school name, or picture to people you meet on the internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted in any way.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage areas, removable media and academy communications are monitored by security systems and staff may review your files and communications to ensure that you are using the system responsibly and legally.

Internet

- You should access the internet only for study or for academy authorised/supervised activities. Activities such as buying or selling goods, checking social media accounts, playing online games, listening to music and watching videos are inappropriate, unless part of your lesson.
- Only access suitable material – using the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- The use and access of social media or online forums is strictly prohibited unless used within a lesson, otherwise these services will remain blocked from access.
- People you contact on the internet are not always who they seem. Always ask a parent/guardian or teacher to go with you if you need to meet someone who you only know from the internet or via email.
- Inappropriate use of the academies computers or network to access explicit content or to undertake inappropriate online behaviour i.e. cyberbullying, harassment, humiliation, intimidation etc is strictly prohibited. Furthermore, this comes under the Online Safety Act 2023. If found to be undertaking any inappropriate online activity covered by the Online Safety Act, the school has a responsibility to act accordingly from removing access to even informing the authorities.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with the existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.