Avonbourne Boys' & Girls' Academies
The best in everyone™
Part of United Learning

Computer and Internet Acceptable Use Policy

The Internet is a global network of computers that communicate with one another, enabling access to a vast range of educational resources.

Avonbourne Academy students can access the Internet as part of their studies, using computers in many areas of the school. It can be a tool of limitless value, providing access to quality educational material from all over the world. The school systems also have a wealth of educational programmes and data held locally.

However, the Internet is also home to a body of material that no parent would wish their child to view. The academy , UL and our Internet Service Provider provides a filtering service, which aims to ensure that none of this information can be accessed, and users cannot interact with others on the Internet who may not be who they claim to be. The filtering service cannot be guaranteed to be 100% accurate. Consequently, users need to be aware of how to use the Internet and other school systems safely, legally and appropriately about their own and others welfare. This Acceptable Use Policy outlines how users should, and should not, use the computer and Internet facilities provided by the academy.

Avonbourne Academies monitor and record user's computer and network activities, and the data that they access and store, to help guard against inappropriate or illegal use.

All users shall:

1. Always ensure that when they have finished working on a computer, they log off properly and leave the equipment as they would expect to find it
2. Ensure E-mails are polite and contain all the usual levels of courtesy associated with a letter or direct conversation
3. Report any breaches of the requirements in the following section to a member of teaching staff, who will inform the relevant Head of Department and the E-Safety Coordinator as appropriate
4. Report any inappropriate site or material discovered on the Internet to a member of teaching staff, who will inform the Head of Department and the E-Safety Coordinator. Staff users should also refer to the Whistleblowing Policy where appropriate

All users shall not:

1. Play games on the school computers or Internet during lesson time, except for educational purposes associated with lessons
2. Dismantle, damage, disable or remove parts from computers or network equipment (e.g. mouse, keyboard, cables)
3. Intentionally waste resources (e.g. excessive printing, unnecessary e-mails)
4. Use school systems for commercial purposes (buying and selling)
5. Eat or drink near computer equipment

6. Engage in ‘Chat’, ‘Chatroom’ or Social Networking (Facebook, Twitter, etc) activities on the Internet
7. Give any of their own, or pass on other people’s personal details (school, address, email, phone no., picture, etc.) on the Internet
8. Arrange to meet anyone over the Internet
9. Disclose their password to others or use passwords intended for others. Users are responsible for all actions performed using their Logon ID
10. Attempt to guess other user’s passwords, bypass security in place, hack into, or alter settings on computers or the network
11. Attempt to gain access to areas of the system for which they do not have the appropriate permissions
12. Use any hacking or key/code cracking software, or hardware
13. Promote or attempt to spread viruses or any other malicious computer code/programmes
14. Download computer programmes
15. Attempt to use or install any programmes other than those installed on the system by the school
16. Breach copyright law relating to computer software, music, video or other copyrighted material
17. Create folders, use filenames, create documents or send e-mails that use offensive language
18. Send, download or post any data, files, attachments, or pictures that contain offensive, falsified or illegal material
19. Visit inappropriate sites, or download inappropriate material, such as those that may contain pornographic, violent, racist, hacking, illegal or offensive materials
20. Use proxy bypass sites to bypass school Internet filtering
21. Attempt internet access using equipment such as a dongle
22. Store their own music, video or other data on the school network, unless it is specifically for educational use
23. Send or forward e-mails that contain pornographic, violent, racist, bullying, threatening, hacking, illegal or offensive language or materials
24. Send or forward spam, chain, junk or nuisance e-mails
25. Use any email (e.g. Hotmail, Yahoo, etc.) or Instant Messaging (IM) system other than those provided by the school
26. Attempt to connect their own personal laptop, PDA or any other device via cable, wireless, or any other means to the school network. Internet connection will not be available for any device which is not part of the school network
27. Ignore any ‘Virus Detected’ message, or fail to act on the instructions within it

28. Use their school email address for any purposes (such as logging onto social networking sites) not associated with school or school work

The use of school computer systems and the Internet will be monitored and recorded, and this information may be passed to other relevant authorities (e.g. the Police) if any illegal activity takes place. This information is based on the user's Logon ID and password.

Misuse of school computer systems or the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion.

Any breach of the above will be sanctioned under our behaviour system rules. A warning letter will be issued on the first occasion and an SLT detention on the second occasion in a period of a term. We reserve the right to remove a student's access to the internet for continued violations of the Acceptable Use Policy.

Any internet search which causes concern will be referred to our Safeguarding Team immediately.

Please keep this policy for your reference

Date of last review	January 2022	Review period	1 Year
Date of next review	January 2023	Author	J Goldsmith
Type of policy	Statutory	Approval	S Ingram 17.1.2022
Signature			
Date of this review	January 2023	Review period	1 Year
Date of next review	January 2024	Author	J Goldsmith
Type of policy	Statutory	Approval	M Dyer 9.2.2023
Signature