



POLICY DOCUMENT FRONTPAGE

ICT Acceptable Use Policy – Student Guidelines

CURRENT POLICY

APPROVED BY ALEC HUNTER LOCAL GOVERNING BODY

**THIS POLICY IS REGULARLY REVIEWED FOLLOWING
RECOMMENDED GUIDELINES**

ICT ACCEPTABLE USE POLICY – STUDENT GUIDELINES

The school has broadband connection to the internet. The internet is a valuable resource to all students which helps them with their learning in all areas of the curriculum. However, as anyone can add information to the internet, there is some material which is unsuitable for viewing by children. We have, therefore, introduced procedures which should enable your son/daughter to use the internet safely and securely. A filtering programme has been installed which should deny access to unsuitable material and the school has an Acceptable Use Policy which is strictly enforced. We will make every effort to ensure unacceptable material is not viewed by your son/daughter and all students and staff users of the internet must agree to follow the rules set out in the Acceptable Use Policy below

The ICT Acceptable Use Policy is an agreement between the parent/carer, their child and the school to use the internet for educational purposes only. Its aim is to:

- Allow all users to access and use the internet for educational purposes.
- Protect employees and students from sites, information and individuals, which could undermine the principles, aims and values of Alec Hunter Academy
- Provide rules which are in accord with the General Data Protection Regulations.

Equipment

- Students must not download or install software on school technologies.
- Viewing, uploading, downloading material for private use (music/film/games) into the school account is not permitted. This applies to any material of a violent, dangerous, racist or of inappropriate sexual content or which is likely to be offensive.
- It is not permitted to transfer inappropriate material from any source into the school user area, or onto any storage media or device to bypass the school filtering system.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts student work at risk and could result in the school applying sanctions in accordance with its Behaviour for Learning Policy.
- The ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. must only be used for school purposes.
- Students are encouraged to use One Drive for the purpose of sharing documents between home and school. In the event that a student needs to use a personally owned removable storage media device, they must first seek permission from a member of staff.
- Eating or drinking in ICT rooms is forbidden.
- Students should always make efforts not to intentionally waste resources, including, but not limited to, excessive use of computer printers without checking "Print Preview" on screen first, excessive storage or unnecessary files on the network storage areas.

Security and Privacy

- Students must protect their work by only logging on to the school network with their own username and password. Using someone else's account for any application or using someone else's name or password is completely unacceptable and will result in the school applying sanctions in accordance with its Behaviour for Learning Policy.
- The school's ICT security system must be followed, and passwords should not be revealed to anyone. Students should change their password regularly.
- To protect themselves and the systems, students should respect the security on the computers. Any attempt to bypass or alter the security settings is forbidden.
- Students must never reveal their home address, telephone number, school name, picture or any other identifying features to people they meet on the Internet.
- Taking or publishing images/video/audio recordings or other identifying media of students and/or staff without the express permission of a senior member of staff is forbidden. Images/video/audio recordings or other identifying media will only be stored and used for school purposes in line with school policy and will not be taken outside the school network or used outside of official school platforms without the permission of the Headteacher.
- Other computer users should be respected and should not be harassed, harmed, offended, or insulted.
- All use of the school's internet and email in school, away from school and at home, whilst using the school systems, is recorded and the logs uploaded to the school system. Personal user areas on the network will also be monitored on an ad hoc basis to ensure adherence to policies and the law.

- Attempting to delete or alter the work of others without their consent is strictly forbidden and will result in student(s) being banned from the school network, as well as other consequences.
- Students must respect the privacy and ownership of others' work at all times.

Internet

- Students should access the internet only for study or school authorised/supervised activities. This applies during and out of lessons. Private use of the internet during the school day is strictly forbidden, this includes any attempt to use any social networking sites which is forbidden on school ICT equipment.
- Students should exercise caution when researching sensitive subjects; they ask their teacher for advice and not seek to disturb or frighten others if they find a subject upsetting.
- Students should 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. If a student accidentally accesses any such material, they must report it immediately to a teacher.
- Students must respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Cyberbullying is a criminal offence and may be reported to the Police. We will follow our Behaviour for Learning Policy in response to cyber-bullying. If a student is the victim of cyber-bullying, they must report it to a member of staff. Students can also report cyber-bullying by using our CEOP button found on the school website.
- Abusive e-mails, inappropriate pictures and any contact by unknown persons to the school should be reported.
- It is essential that any incidents of offensive or bullying behaviour online are immediately reported to a teacher.
- In addition, students who are subjected to any incidents of a sexual nature must press the CEOP report button on the school website homepage.
- All electronic communication with staff at the school must be conducted via the school's e-mail system or website **and not** social network sites (Facebook etc). Students must **not** communicate with staff via personal e-mail.
- Language used in electronic communication must be appropriate and suitable, as for all schoolwork. Students must communicate in a respectful manner with staff and must not ask any questions of a personal nature.
- Students must **not** send or forward messages, publish or create material, which is offensive, hurtful, or otherwise upsetting to another person or which has the potential to damage the reputation of the school.

Email and other School Communications

- Students are only permitted to use their own official school e-mail account, which must be used in an appropriate manner. Students must not send abusive mail, use inappropriate language or send attachments which are deemed inappropriate or offensive. Students are not permitted to use any other e-mail service.
- Students use Microsoft Teams to support their education and learning. In doing so, students must ensure they use the features of Microsoft Teams appropriately.
- Students must be polite and appreciate that other users might have different views from their own. The use of strong language, swearing or aggressive behaviour is as anti-social on the internet as it is in the street. Doing so will result in being banned from the network and could result in the school applying sanctions in accordance with its Behaviour for Learning Policy.
- Students should only open attachments to e-mails if they come from someone they already know and trust. Attachments can contain viruses or other programmes that could destroy all the files and software on the computer.
- If a student receives an e-mail containing material of a violent, dangerous, racist, or inappropriate content, they must report such messages to a member of staff. The sending or receiving of an e-mail containing content likely to be unsuitable for children is strictly forbidden.

Copyright

The school has a Copyright Licensing Agency (CLA) Education Licence, and this means:

- Students can copy works in any medium as long as it is just for schoolwork and other activities within the school. The student must acknowledge where they got the copied work from (display the web address, book title and author etc).
- The audience of the copied works must be limited to teachers, pupils and others directly connected with the activities of the school.

If a student fails to observe these guidelines, action will be taken by the school in line with the Behaviour for Learning Policy. For serious violations, a ban from using ICT facilities or an exclusion may be imposed. Where appropriate, Police will be involved, or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.