Ashton Community Science College

ICT Security (Students) Policy

Version Control

Named Owner:	Mrs S Evans / Mr T Bleasdale / Mr S Patel
Version Number:	1.00
Date Of Creation:	
Last Review:	January 2024
Next Scheduled Review:	January 2027
Overview of Amendments to this Version:	Mr T Bleasdale – new IT Manager

Network, E-mail and Internet Use Good Practice

Rules for ICT Use

The school computer system provides Internet access to students for the sole purpose of learning. This Network, E-mail and Internet Use Good Practice statement will help protect students and the school by clearly stating what is acceptable and what is not.

- School computer and Internet use must be appropriate to the student's education.
- Access must only be made via the user's authorised account and password, which must not be given to any other person.
- Users must take reasonable precautions to ensure no computer viruses are introduced to the network, when transferring schoolwork from portable storage devices.
- Copyright and intellectual property rights must be respected.
- Users must respect the work of others, which might be stored in common areas on the system. Conversely, users should always try and store their files and data in their own secure area or on removable media. Files and data stored in common areas of the system must be transferred at the earliest opportunity to the user's own area. Such files will be regularly removed from the system. Games are not allowed to be saved in user areas or common areas.
- Users are responsible for any e-mails they send, and any messages sent on Microsoft Teams. Both should be written carefully and politely. As messages may be forwarded and postings will be read by other students and staff, they are best regarded as public property. Anonymous messages and chain letters must not be sent.
- Users should report any unpleasant material or messages received. The report will be confidential and will help protect others.
- The use of public chat rooms is not allowed.
- The school ICT systems may not be used for private business purposes, unless the headteacher has given permission for that use. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Irresponsible use may result in the loss of Internet access.
- Any faults with I.T. equipment must be reported to a member of staff.
- Users must take care of I.T. equipment and surrounding workstation.
- No food or drink is to be consumed whilst in the vicinity of I.T. Equipment.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of all web traffic, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unsuitable, unauthorised or unlawful.

Cyber Bullying – Code of Conduct

- If you feel you are being bullied by email, text or online within school, contact a member of staff.
- Never send any bullying or threatening messages. Anything you write and send could be read by an adult.
- Serious bullying should be reported to the police - for example threats of a physical or sexual nature.
- Keep and save any bullying emails, text messages or images.
- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.
- Why not log into a chatroom with a different user ID or nickname? That way the bully won't know who you are. You could change your mobile phone number and only give it out to close friends.
- Contact the service provider (mobile phone company, your internet provider) to tell them about the bullying. They may be able to track the bully down.
- Use blocking software - you can block instant messages from certain people or use mail filters to block emails from specific email addresses.
- **Don't** reply to bullying or threatening text messages or emails- this could make matters worse. It also lets the bullying people know that they have found a 'live' phone number or email address. They may get bored quite quickly if you ignore them.
- **Don't** give out your personal details online - if you're in a chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.
- **Don't** forward abusive texts or emails or images to anyone. You could be breaking the law just by forwarding them. If they are about you, keep them as evidence. If they are about someone else, delete them and don't reply to the sender.
- **Don't** ever give out passwords to your mobile or email account.
- **Remember** that sending abusive or threatening messages is against the law.

Adapted from Anti Bullying Network