

## STUDENT ACCEPTABLE USAGE POLICY

- The school allows you to use the computers and other devices in school to access the Internet to help you with your learning. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment.
- You will only use the ICT systems and other devices for school work and homework. You should seek permission first for any other use.
- You should keep usernames and passwords safe and do not reveal these to anyone else. Only log on using your own account.
- You should not deliberately search for, view, download, upload or forward material that is illegal or that would be considered offensive by another user. This includes content that is pornographic, racist or violent in nature.
- If you encounter any content or communications that is unpleasant or upsetting, or you believe is illegal or would be considered offensive by another user, you should report this to a member of staff immediately.
- Only send messages to people you know, using your school email address or other school-created accounts. Other contacts should be agreed with a member of staff before messages are sent.
- Any messages you send, content you post online or work you create using the school ICT systems must be polite and responsible. It is not acceptable to harass, offend or cause upset to any other user. This includes taking or creating digital photos or videos of other staff or students without their consent.
- Any messages you send or posts you make to websites, in or out of school-time, should not cause staff, students or other users distress or bring the school into disrepute.
- You should not give away any of your personal information, or the personal information of other users in school, over the Internet. This includes photographs or video images of yourself, other students or members of staff.
- You will not arrange to meet someone you only know online unless this is part of schoolwork, in which case you will inform a member of staff and will ensure a responsible adult, parent/carer goes with you.
- You should respect intellectual property and ownership of online resources you use in your schoolwork, and ensure you acknowledge all sources you use.
- You should not attempt to change any settings or install any software on equipment without permission. You should ask permission from a member of staff before downloading files or resources from the Internet.

- You should not attempt to bypass any security, filtering or monitoring systems that may be active on equipment. They are there for your protection and safety. If you feel a legitimate resource is being accidentally blocked you should ask a member of staff to investigate for you.
- You should check any files brought in on removable media, such as USB sticks or CDs, to ensure they are free of viruses and other malware before use. Files brought in from home should only be directly related to school work.
- You should not connect any personal equipment such as mobile phones, cameras or media players to the school ICT system, or attempt to access the school network from any personal equipment, unless this is part of an educational activity and you have permission from a member of staff.
- You should not attempt to access or delete resources, files or messages belonging to someone else.
- You should not waste valuable time and resources on activities that are not directly related to school work.
- The school will ensure you receive regular eSafety information and guidance, and you will take an active responsibility in assessing the potential risks of the technology you use, and for using such technology (in and out of school) in a safe, responsible and legal way.
- You understand that your files, communications and Internet activity will be monitored and checked at all times. If these statements or other guidance from the school are not followed, action may be taken to protect yourself or others, including restricting your access to the school ICT systems. In certain circumstances it may be necessary to confiscate personal equipment to protect yourself and other users.