COMPUTER RESOURCES GUIDELINES

Privacy

- Computer (file) storage areas will be treated as school property.
- Staff may look at files and communications to ensure that the system is being used responsibly, users should not expect that their work and emails will always be private.
- Students should also be aware that a member of the computing staff can view their computer screen at anytime from anywhere on the school network without them knowing about it.

Students should note the following guidelines:

- Do not install, attempt to install or store programs of any type on the computers without permission.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as memory sticks, CDs, flash drives, etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs, etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security

- Only use your school email address and do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet your home address, your telephone number, your school's name, or send them your picture, unless you are given permission to do so.
- Do not use the computers in a way that harasses, offends or insults others.
- Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Do not attempt to infiltrate the school’s internal network infrastructure.
- Do not attempt to run third-party software from USB storage devise
- Do not attempt to scan or gain access to the school’s network infrastructure in any form. The school’s system is configured to track and trace breaches of protocol and can be treated as a criminal offence
- Do not attempt to physical connect any devices to the school’s network

Internet

- Do not access the Internet unless for study or for school authorised/supervised activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities over the Internet. This takes up valuable resources which could be used by others to benefit their studies.
- Never arrange to meet anyone unless your parent/carer or teacher goes with you. People you contact online are not always who they seem.

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 not allowed.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.
- The sending or receiving of emails containing material likely to be unsuitable for children or school is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content

Additional action may be taken by the school in line with 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.

The daily use of the schools computing network is provided by the school to facilitate teaching & learning and is treated as a privilege to use, not a right. If the school’s rules or protocol are broken access to these resources can be revoked at any time. All systems are monitored, logged, and audited on a regular basis.