



Bacup & Rawtenstall Grammar School

Student Acceptable Use Policy - Network and Internet Access

This Agreement summarises the standard of acceptable behaviour that is expected from all BRGS students when using the network. Any student who is considered to have broken any of these terms will be reported to his/her Head of Year in the first instance and may be refused access to the network until sanction has been agreed. In severe cases, access to the network may be withdrawn permanently.

The school network and Internet is provided to assist you with your SCHOOL WORK. Personal files should not be stored and, if found, will be removed. This includes personal photographs.

Students are responsible for everything carried out under their login. Please ensure no one else has access to your computer when you are logged in as **you** may be held responsible for **their** actions.

Passwords and accounts must never be shared. Please change your password regularly.

Students who wish to transfer files to and from school are advised to use DROP BOX. (User instructions can be found on the shared area of the network in the 'How to.....' folder).

USB flash drives or other similar devices are not allowed on the school system.

Students **should not attempt to download toolbars, programs or other items** to the network.

Any student **found attempting to circumvent the school or county council's filtering** in any way will be reported to the headmaster and may have network access withdrawn on a permanent basis.

Students are responsible for ensuring any **files they transfer onto the school network are free from viruses and adware.** Any **clean up costs incurred** as a direct result of such malware being brought in by students **will be passed on to pupils and/or their parents.**

Copyright of material must be respected at all times.

Students should never attempt to fix faults with ICT equipment themselves. Any faults with computers or associated equipment should be reported to the class teacher or supervisor.

Vandalism of school equipment is taken very seriously. Anyone found to be responsible for damaging ICT equipment will be reported to the Headmaster and invoiced for the cost of repair/replacement. Anyone discovering or witnessing acts of vandalism is asked to report it, in confidence, to a member of the Network Team

Network monitoring software is in place and covers users whether **on or off the Internet.** Screen shots are taken regularly. In addition, the network team may choose to view any screen in a live session at any time.

Students **should not chat to other users on the network or send personal e-mails** whilst connected to the network. Only e-mails relating to school work should be sent in school.

Please remember that, **should you ignore the regulations** and open personal mail in school, monitoring software **may make it possible for staff to read your personal e-mails.**

The **security of ICT systems** whether owned by the school or by other organisations or individuals, must not be compromised in any way by a student's actions.

All instances of inappropriate websites, messages or other material found on the school system should be reported, in the first instance, to the class teacher.

NB: IN YEARGROUPS WHERE STUDENTS LEAVE SCHOOL BEFORE THE END OF THE ACADEMIC YEAR IN ORDER TO REVISE FOR PUBLIC EXAMINATIONS, THIS POLICY WILL REMAIN IN EFFECT UNTIL THE END OF THAT ACADEMIC YEAR. FOR ALL OTHER YEARGROUPS THE POLICY REMAINS IN FORCE UNTIL AMENDED OR CANCELLED BY SCHOOL.