

Acceptable Use of Information Technology Resources at Bordertown High School

Policy

The comprehensive computer network at Bordertown High School supports the teaching and learning program and is intended to extend students' learning. As a student of Bordertown High School, your access to the computer network will enable you to complete course work and develop skills using our IT resources.

Responsibilities

Each student has a responsibility to take care of the computing resources and use them in a careful and constructive way. It is essential that you:

- logon to the network using your own account only
- leave all equipment in place unless you have teacher permission to do otherwise
- report equipment problems - do not tamper with systems settings, switches, buttons or cables
- logoff from the network and leave the work station area neat and tidy at the end of your session
- ensure enough personal internet and print credit is available to complete all curriculum work.
- do not modify any desktop settings.

User Name and Password

Each student will be allocated an account (User Name and password) to access the network resources. This will give the user access to:

- their own secure server storage space
- all networked printers
- the internet through a high speed filtered connection
- personal (electronic mail) email account
- controlled quantity of Internet downloads.

The password protects your storage space and Internet access. Its confidentiality is your responsibility - do not divulge it to anybody.

The school maintains comprehensive monitoring and logging procedures. To ensure security, integrity and responsible use of the resources and as part of maintenance, systems management will monitor all student activity, particularly Internet activity and storage space.

Saving

As part of your enrolment you will receive some server storage space. This will be available from any networked computer within the school. All computer work carried out at school should be performed and saved within the server storage area. ***Students are responsible for managing folder space by periodically deleting unwanted files.*** Under no circumstances will a student store executable (.exe) files, music files, video files or other files not related to subject content. On our server your files will be backed up weekly but ultimately each user is responsible for their own files. ***The school does not accept responsibility for a failed backup.***

Floppy Disks/Flash Drives and Viruses

Flash drives are a major source of viruses into the network. You should use a flash drive *ONLY* if you need to transfer school-related work files to and from home for further development and as a backup. Flash drives can be unreliable. All our files may be checked for virus contamination before they are opened. Management reserves the right to check any flash drives within the school and confiscate those that pose a threat to the performance of our resources. The school updates its virus software very regularly but gives no guarantee that it is 100% virus free at any point in time. If you use a flash drive on the school network you may be asked to display the contents to Systems Management.