CODE OF CONDUCT - For computer usage.

Asquith Boys High School has an extensive network of computer equipment including almost 200 computers, several data projectors, interactive white boards, printers, scanners and video conferencing equipment. Students from Years 9 to 12 also have access to DER laptops.

Student have certain rights and responsibilities in relation to the use and care of this equipment. A high standard of behaviour and cooperation is expected at all times. Students must understand that the computer network is a shared resource that contains information belonging not only to them but also to other students, teachers and clerical staff. Much of the data on the system is vital for the operation of the school and students must not do anything that would place the data at risk.

Students have the responsibility to:

1. Only use the computer system for its intended purpose:
   - The computer system has been provided by the State Government and the School as a resource to improve the quality of education provided at the school.
   - The computers are not provided for entertainment. This means students must not bring to school, or download, or play directly from the internet, any games, music, videos etc.
   - Students must not use the computers to harass or bully other people.
   - Students must obey the code of conduct set out by the DET for internet usage. This relates to the use of only appropriate sites.
   - Students must not bring computer equipment such as external hard drives and notebook computers from home. Students are permitted to transfer files via email and on small USB flash drives but there should be no reason to bring external hard drives.
   - Personal notebooks are also not permitted since most are capable of accessing the internet via external suppliers, thus bypassing the DET internet filtering system. We are not permitted to allow this to happen. Multiple computers have been provided for student use at school. There is no need to bring computers from home.

2. Look after the computer hardware:
   - Do not enter a room containing computer equipment including interactive white boards and projectors unless a teacher is present to supervise you.
   - Do not do anything that could damage the computer equipment. While all equipment is covered by a warranty, that warranty does not extend to deliberate damage of equipment. If equipment is deliberately damaged it will be removed until it can be repaired. If the student who damaged the equipment can be identified, they will likely be expected to make restitution.
• Do not move equipment around. If a mouse, keyboard or monitor is not working, don't try to fix it by moving equipment, just report the problem and move to a working computer.

• All computers are locked or bolted to the desks for security. Do not make any attempt to break into the locks. If the code is worked out by students then obviously the codes on all the locks will need to be changed to secure the computers again. This is a costly and time consuming exercise. Students responsible for the problem will likely be expected to contribute financially to solving the problem.

3. Protect the integrity of all data on the system.

• Data in the form of operating systems, programs and files is the most valuable part of the system. Files belonging the HSC students, staff members and containing financial information about the school for example are all stored on the school server. Students must not do anything that could place the data at risk of loss or theft.

• Student are responsible for protecting their own data. While the school does have a backup system, it is often affected by students who store large amounts of data on the server. This often prevents the backup operating correctly. Students should backup up their own files for safe keeping. USB Flash drives are permitted for this purpose. The school will also try to protect student's work by backing up their files, but we take no responsibility for any lost data that may occur.

• Student must not allow other students to use their accounts by either logging them onto the computers or by giving out their passwords. If you have forgotten your password it is easily retrieved by using your "Secret Question" or be asking a teacher to reset your password. Students are responsible for all files stored in their home folders.

• Any student who brings files to school or who downloads files for the purpose of breaking into the computer system will immediately have his computer account closed. The account will not be re-established unless the student can convince the school that this will never happen again.

• Students may not store non-school related files on our server. No executable files, games, music, or videos should be stored on the school system as these files are of no educational value and in large numbers they will affect our backups. Videos, images and audio files created at school as class activities and assessments can be stored although they should be removed once the activity has concluded.

• Students have been known to create large numbers of embedded folders in order to hide files. The creation of a large number of embedded folders not permitted as this also affects our backups.

• Students may not attempt to load program onto any computers at school due to a real risk of virus infection from their files as well as the likely breach of copyright laws.

   **Remember the use of the computer system is a privilege not a right.**