



Electronic Devices Policy

The following policy is to be used in conjunction with the MacGregor State High School Responsible Behaviour Plan for Students and the MacGregor State High School Prevention and Responses to Incidences of Bullying including Cyberbullying.

DISRUPTION OF CLASSES

MacGregor has a zero tolerance policy for misuse of mobile phones or electronic devices, including ear plugs/headphones for a device, being seen, used or heard during class time. The simple rule is “turned off and put away”.

On some occasions teachers will permit the use of devices in class for clear educational reasons (this does not include listening to music while doing other work). The teacher will explicitly explain the parameters for use of the device and will enact the Responsible Behaviour Plan steps if these parameters are breached.

Mobile phones are not permitted to be charged at school.

Under no circumstances will the school accept responsibility for the loss of any personal items.

In the event of a student being seen in possession of a device, using a device or having their device make a noise such as a text alert or alarm during class time, the staff member will follow the steps in the Responsible Behaviour Plan for Students.

MacGregor has a zero tolerance to Cyberbullying (see associated Cyberbullying policy).

Consequences for inappropriate use will range from a warning to after school detentions to suspension from school depending on the circumstances surrounding the incident.

During exams electronic devices are to be turned off and kept in school bags.

MACGREGOR SHS NETWORK USAGE AND ACCESS GUIDELINES

The school computer network (including internet and email access) is provided to students for educational purposes only.

EXPECTATIONS OF STUDENTS

Username and Passwords:

You have been issued with a username (account) and password that are for your use only.

Passwords must be over 7 characters in length and must include a mix of letters, numbers and symbols (! ? \$). For example – Ex@mp1e!

The system will require you to change your password regularly. You cannot use any of your previous 13 passwords. Try not to use words that could easily be guessed by other students.

Never let anyone know your password. If you believe someone has your password, your teacher can reset it.

If you forget your password, ask your teacher to reset it.

Use of the Internet:

Education Queensland provides a managed internet service to students. Filtering is in place to provide safe and secure browsing to appropriate web sites. Let your teacher know immediately if you find an inappropriate site.

Attempting to bypass internet filtering (or searching for means to do so) is a serious breach of school computing rules. If you encounter any emails or web sites offering to bypass security (proxy sites), inform your teacher immediately.

All internet activity is tracked by the filtering service and logged. These records may be accessed by school administration at any time. Inappropriate internet use will result in your access being suspended.

Maintain your privacy at all times. Never reveal your home address, phone numbers or photo on internet sites. Do not reveal these details of other students either.

In order to maintain equitable access for everyone, a monthly download limit of 1000MB is provided to students.

Acceptable/ Appropriate Use/Behaviour by a Student:

The use of computer and Internet resources at Macgregor SHS is a privilege not a right. Inappropriate use will result in suspension of those privileges. Additional disciplinary action will be taken in line with the MacGregor SHS Responsible Behaviour Plan for Students Step Process.

Do not search for or try to access sites relating to pornography, graphic violence or terrorism.

You accept personal responsibility for your behaviour while using the school's computer facilities. It is important that you do not loan your network username to another student as you are accountable for all activities conducted on your account.

Report any misuse or damage of the computer network by others to your teacher. Misuse includes vandalism, theft, security breaches or inappropriate use of email or the Internet.

You must not copy any school software. To do so is regarded as theft. Nor can you install or run software on school computers.

Use of software programs, apps or internet sites (including email) during class time must be approved by your teacher.

Each computer laboratory has guidelines and procedures for computer use including logging on and off, printing, software and hardware use and what can be brought into the room. It is your responsibility to be aware of and to follow these guidelines.

Secure your work - some students may wish to copy or delete your work. Ensure all work is saved two places (eg. H: drive and USB).

Ensure you log off the computer at the end of each lesson. Do not leave your computer for a long period of time without locking the screen. See your teacher if you find a computer left logged on.

Social media sites like Facebook, Twitter or Instagram are not permitted at school.

Web based chat rooms and mailing group services are not to be accessed at school.

Cloud storage like Dropbox and Google Drive are currently blocked at the request of the Education Department due to security concerns.

Use of Email:

You have been provided with a school email address to use for everything related to your studies, not for social or chain messages.

Only use your school provided email while at school. Web based email services like Hotmail or Gmail should not be accessed at school.

Email is a very useful communication tool - always be polite and use appropriate language. Abusive or vulgar language (swearing) and violent language will trigger the filters to report you to administration, and further action will be taken in line with Set Process.

Antisocial behaviour or language and harassing other students (bullying) is not appropriate or acceptable.

In order to preserve bandwidth, there is a size limit to email attachments of 5 MB.

BRING YOUR OWN DEVICE. STUDENT EXPECTATIONS.

My device is a learning tool that is used to enhance my classroom experience. My device is to be used at the instruction of my classroom teacher.

Ensure my device is fully charged at the beginning of each school day.

Use my device for educational purposes only, using only apps that I have been instructed to use by my teacher.

Use my device to communicate with others only when instructed by my teacher.

Only use my device during exams when instructed to do so.

Use my device for educational purposes (not gaming). This includes the use of camera and video functions. The use of these is only with teacher permission.

Keep my device safe and secure. Devices should be kept in school bags when moving around campus.

Not share my device. It is my responsibility to keep my device secure at all times.

Communicating with others (communication tool)

My device is a learning tool that can be used communicate with teachers, peers and information within and beyond the school.

Retrieve/browse only information which is relevant, appropriate and acceptable to the school community.

Respect others in all communication, always being aware of my Digital Footprint. This includes all emails, Learning Place discussion boards, Learning Place forums and Learning Place wikis.

Access only my school provided email account when emailing teachers and other students and only communicate using the device when instructed by a teacher.

Only use file sharing abilities (such as airdrop) when instructed by a teacher.

Digital Footprint and Cyber Safety

The digital footprint I leave represents who I am as a person.

Not allow any other student to use my device or personal internet connection. Social media applications are not to be accessed at school.

Back-up all of my school work. Equipment failure is not a valid excuse for not handing in assessment.

Not attempt to connect my device to the school network and its resources in any way.

Maintain the privacy of my home address, telephone number or any credit card or pin number and not disclose any of these details over the internet.

Observe all copyright laws, including those relating to computer software, music and videos.

Refer to MacGregor SHS Prevention and Responses to Incidences of Bullying including Cyberbullying.