A MESSAGE FROM THE PRINCIPAL

Dear Parents/Carers

At Mackay Christian College, one of our goals is to keep our students as safe as necessary while they are connected to the MCC internet system.

To alert students to possible unsafe behaviour, the College has a Student Acceptable Use of ICT Conditions statement (Policy 1S 15) which is attached at the end of this letter.

In Prep to Year 12, parents/carers agree to the conditions of this policy when you sign the Enrolment Contract which states on p. 1:

Relationship
I/We agree to:
- work in partnership with the College in support of College policies and expectations that are available to us either in hard copy (e.g. Student Diaries and other publications) as well as on the College website;
- support and comply with published College policies and expectations ourselves, in the best interests of our child and the other students enrolled at Mackay Christian College;
- encourage my child to uphold College policies and expectations;
- accept that any failure by us or our child in this commitment may lead to serious enrolment consequences;
- accept that we are liable to indemnify the College for any damage that may arise from such breach, including any arising from wilful defiant behaviour of the student or refusal to follow reasonable directions;
- accept that the policies and rules may need to change from time to time in line with the best interests of staff and students. I/We accept that the College is obliged under law and ethos to act in the best interests of the individual student and the student body generally. Although the College values consultation with parents/carers, this may mean that the College may not always act in accordance with your preferences and requests.

Students in Prep to Year 4 are provided access to e-devices and the College internet under the permission and guidance of parents/carers and staff in line with Policy 1S 15.

As well as parental contract consent, students in Years 5 to 12, who we believe are able to understand the implications of the terms of ICT acceptable use, also agree to abide by these conditions with an acknowledgement at the beginning of each year upon first log-in to access the College internet and its resources.

Thank you for supporting your child to understand the safety implications behind the Acceptable Use of ICT Conditions. Though we cannot guarantee the internet filter will not be breached, the College endeavours to have safety and security measures in place to avoid accessing unacceptable sites.

Bless you,
Dr Lesley Tunnah
College Principal

Policy 1S 15

Students enrolled in Prep to Year 12 at MCC who hold a College network account may access the College's network using only approved electronic learning tools and supervised by staff from 8:30am to 3:00pm on school days. Student access to the College network will be granted once the College has received a signed Student Acceptable Use of ICT Agreement.

While the College has programs in place that assist in the filtering of inappropriate material from network sources, parents/carers of students are ultimately responsible for setting and conveying the standards that their child should follow when using media and information sources.

MACKAY CHRISTIAN COLLEGE STUDENT ACCEPTABLE USE OF ICT CONDITIONS:

1. Students who fail to comply with the Student Acceptable Use of ICT Conditions risk being denied access to College ICT services either temporarily or permanently, as well as facing potential disciplinary action. Student users of College technology are personally responsible for their behaviour and communications when using College accounts.
2. All communications on the College network should be approached using the CLEAR Technology at MCC values listed in MCC's Electronic Devices Policy, namely: Care for your computer, Leave a lovely digital footprint, Enjoy the e-adventure with excellence, Always avoid danger and Reliable resources rule.
3. Student access to College technology is granted on a privilege basis. Students are issued with an individual College network username and password for which they are responsible, which includes keeping their password secure. Any unauthorised material accessed under a student's password will be deemed the responsibility of that student. Disregard of this policy may lead to removal of this privilege.
4. Network eDevices storage areas and files stored on College services are not private. At any time College administrators may review files and communications to ensure student users are accessing the network responsibly. Student material stored on servers (e.g. iCloud) which the College cannot readily access remain the monitoring responsibility of parents/carers. Students are responsible for backup of files.
5. Within reason, access to information will be honoured. Teachers will guide students toward appropriate digital material for educational purposes. Outside of and apart from College-directed activities, parents/carers will bear the responsibility for guidance with information sources.
6. Students are responsible for regularly and appropriately backing up their files.
7. Any suspected data breaches are to be reported to the ICT Department.
8. The following activities do not align with the College's values, or Code of Conduct, and are **not permitted**:
   - sending or displaying obscene language or offensive messages, pictures, spam, etc that violate community standards of decency
   - making harassing, insulting or defamatory comments about others or self
   - damaging College eDevices, systems or networks
   - infringing or violating copyright laws including copying and transmitting documents, software, music, games and/or video files without licence or permission
   - using another person's username and/or password **at any time** or accessing another person's files
   - intentionally wasting limited resources or disrupting the network use of another College user
   - access and use of unauthorised sites or loading unauthorised programs
   - listening to or viewing any unauthorised material including music, movies, games, etc
   - using College ICT resources for unauthorised recreational, commercial or political purposes
   - theft of College software or hardware
   - creating 'peer to peer' networks e.g. Bluetooth or wireless connections, or sharing their eDevice's resources for anything other than educational purposes
   - illegal activity in violation of any federal or state laws or regulations
   - distributing private information about others or self in any form, including via emails, photographs, recordings, mobile phones and the internet
   - providing access to the College network resources to unauthorised users
   - cyberbullying, or any other harmful online behaviours
   - installing apps or software on their College eDevice which are deemed inappropriate for College use, including Vault apps, VPNs or unprotected social media
   - plagiarism in any form, including AI.
9. While on campus, any unauthorised privately owned connections to any network other than the College's network via laptops, PDAs, VPNs, mobile phones, iPads, etc (see Electronic Devices Policy at mcc.qld.edu.au) are **not permitted**.