AQUINAS COLLEGE

POLICY 5.7
Cyber Safety

Approved at Board Meeting	**23rd February 2017**
Next Review Due	**2020**

RATIONALE:

To ensure a safe electronic learning environment at Aquinas College maximising the educational benefits of communication technologies while minimising the risks to users.

GUIDELINES:

1. Professional conduct of all staff is exemplary with colleagues, students and parents at all times. The special character and the College Touchstones reinforce this expectation.
2. The school's cyber safety practices are to be based on information contained in the NetSafe® website - https://www.netsafe.org.nz/ which is endorsed by the New Zealand Ministry of Education.
3. The Board supports the right of the College to check communication technology-related work or data of staff, or students, at any time.
4. Use of the Internet and other communication technologies at Aquinas College is to be in accordance with the signed Cyber Safety User Agreements.
5. 'Other communication technologies' include mobile phones and technologies associated with Internet use, included but not limited to digital cameras, web cam and social networking sites. Included, too, are similar technologies still being developed.
6. The communication technologies at Aquinas College are available to staff and students under certain conditions, as outlined in their signed Staff and Student Cyber Safety User Agreements.
7. Assistive technologies for students with special education needs and/or Ministry of Education technology will be guided by staff user access recognising the nature of the Specialist Teacher or designated Teacher Aide role and to fully access technology and resources for curriculum support.
8. Current cyber safety educational material is to be made available to the College community.
9. Disciplinary responses to breaches of cyber safety and/or complaints will follow the Complaints Policy and viewed in line with the Code of Conduct policy, the relevant Collective Agreements, and the Colleges' disciplinary procedures for students.

PROCEDURES:

1. All staff must sign a current Staff Cyber Safety User Agreement.
2. All students must read and sign a current Student Cyber Safety User Agreement each year. The agreement must also be signed by a parent/caregiver.
3. Cyber safety educational material will be provided by management to staff and students, and to parents/caregivers. Basic training for staff will be the responsibility of the professional development and ICT Groups, annually reviewed.
4. The College will provide an effective electronic security system.
5. The College will continue to refine methods to improve cyber safety.

(To be reviewed by Ray and Jono)

APPENDIX 1 AQUINAS COLLEGE CYBER SAFETY PROCEDURES AT 2014

To be updated and reviewed annually by the ICT Group at the commencement of each school year, alongside the annual review of the *Staff* and *Student Technology Access and User Agreement* forms in keeping with the latest version of the NetSafe® Kit for Schools. (These procedures may be used as the basis for the cyber safety programme)

1. All students must read and sign a ***Student Technology Access and User Agreement*** outlining the regulations and conditions under which computers and communication technologies may be used while at school or in any way which affects the safety of the school learning environment. The agreement must also be signed by a parent/caregiver.
2. Students will be supervised while using school facilities; the degree and type of that supervision may vary, dependent on the type of technology concerned, where the equipment is physically situated and whether or not the activity is occurring in the classroom.
3. All staff must sign a ***Staff Technology Access and User Agreement*** which includes details of their professional responsibilities and the limits to their own use of the Internet.
4. Safety education will be delivered, where relevant, through teaching programmes.
5. The school will make basic training available for staff using these technologies. Associated professional development needs will be considered.
6. Basic training for staff will be made available by management, as will appropriate professional development.
7. The necessary procedures will be put into place by the school to address cybersafety issues in all venues where the Internet and other communication technologies are accessed by staff or students.
8. The school will provide an effective electronic security system, which is financially practicable.
9. The school will continue to refine methods to improve cybersafety.
10. The Principal will be responsible for the establishment and maintenance of a cybersafety programme in the school. (The Principal may well delegate that responsibility to a member of the Senior Management Team.or ICT Group)
11. The Board supports the right of the school to check communication technology-related work or data of staff or students at any time, and to carry out a comprehensive investigation of any breaches of the school's Cybersafety policies. Such breaches will be taken seriously and be dealt with through the school's disciplinary and support systems. In such incidents, there will be special attention paid to the need for specific procedures as regards the gathering of evidence. If illegal material or activities are suspected, the matter will be reported to the Police or the Department of Internal Affairs Censorship Compliance.
12. The school will consult with the wider school community and provide opportunities to learn about cybersafety issues e.g. through Parent Information Evenings.