FSAC Ltd

Board Policy No. 5
Student Welfare

Student Cyber Safety Procedure No. 5.4

St Johns Anglican College
2017

Document Approval and Version Control	
Version # 2.1 Last amended 16.12.2016	Approved by: Head of College Name: Signed: Date:
Contact Officers: Position: Manager Human Resources Name: Craig Middleton	Next Review: 30.06.2017

1. POLICY STATEMENT	Board Policy No. 5 – Student Welfare
2. PROCEDURE STATEMENT	***The Colleges are committed to the establishment and maintenance of a cyber-safe College environment which ensures that exposure to inappropriate material or attention from other users is minimised.***

SPECIAL NOTE: This Policy should be read in concert with Policy No. 2 Student Protection in Anglican Schools policy and procedure. These Student Protection policy and procedures must be kept at the forefront when considering and implementing the contents of this policy and associated procedures. In the even that reasonable suspicions that harm, and/or sexual abuse has occurred or is likely to occur, the Student Protection Policy and Procedures must be followed.

2.1 Scope

This procedure applies to all staff and volunteers of the Colleges.

2.2 Principles

The responsibilities for safe healthy environments for student teaching and learning and the use of the Internet and Information Communication Technologies (ICT), and related cyber safety issues have become increasingly linked.

The following key principles guide the use and application of Internet and information Communication Technology in teaching and learning:

- The Internet and ICT devices/equipment bring great benefits to the teaching and learning program, and to the effective operation of the College.
- The Board places a high priority on providing the College with Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the college.
- It is recognised that the presence in the learning environment of these technologies, some provided partly or wholly by the College and some privately owned by staff, students and other members of the College community, can also facilitate anti-social, inappropriate, and even illegal, material and activities.
- The College has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

2.3 Affiliated Authorities

The following legislation, awards and agreements will be applied:

- NetAlert programme (www.netalert.gov.au)
- *Privacy Act 1988 (Commonwealth)* – incorporating Amendments 2004;
- NetSafe® Kit for Schools
- *Child Protection Act 1999*
- *Anti-Discrimination Act 1991*
- Office of the Children's eSafety Commissioner (www.esafety.gov.au)

3. SPECIFIC DEFINITIONS

Cyberbullying: Is the use of technology for harassment, impersonation, denigration, trickery, exclusion and stalking.

Social network sites: Such as MySpace, Facebook, Google + are services that use the Internet to create an interactive network of photos, videos, blogs etc. Social

networking sites gather data submitted by members as “profiles”, profiles can then be shared among members.

Inappropriate content: Has been defined as visual depictions that are obscene, child pornography, or material "harmful to minors". It can also include images of violence, hate group or extremist material, illegal activities and online advertising.

Cyber predator: Uses the Internet to hunt for victims to take advantage of in ANY way, including sexually, emotionally, psychologically or financially. Cyber predators know how to manipulate children, creating trust and friendship where none should exist

4. APPLICATION

The Colleges’ Cyber Safe environments will be based on the latest version of the *NetAlert* programme (www.netalert.gov.au) developed by the Australian Government and the NetSafe programme for colleges, endorsed by the New Zealand Ministry of Education. *The NetSafe® Kit for Schools.*

5. ICT USE AGREEMENTS

No individual may use the College Internet facilities and College-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the College. **ICT Use Agreements** also apply to the use of privately-owned/leased ICT devices/equipment on the college site, or at/for any college-related activity, regardless of its location. This includes off-site access to the college network from college or privately-owned/leased equipment.

The College **ICT Use Agreements** will cover all employees, all students, and any other individuals authorised to make use of the college Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the college.

The **ICT Use Agreements** are also an educative tool and should be used as a resource for the professional development of staff.

Signed **ICT Use Agreements** will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices/equipment

5.1 Use of ICT Resources

Use of the Internet and the ICT devices/equipment by staff, students and other approved users at the College are to be limited to educational, professional development, and personal usage appropriate in the college environment, as defined in individual use agreements.

5.2 Right to Monitor

The College has the right to monitor access and review all use. This includes personal emails sent and received on the College’s computer/s and/or network facilities at all times.

5.3 Right to Audit

The College has the right to audit at any time any material on equipment that is owned or leased by the College. The college may also request permission to audit privately owned ICT devices/equipment used on the College site or at any college related activity.

6. CONFIDENTIALITY

Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Australian Privacy Act 1988.

7. SUMMARY

The safety of children is of paramount concern. Any apparent breach of Cyber Safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the College's Cyber Safety practices. In serious incidents, advice will be sought from an appropriate source, such as the Australian Communications and Media Authority and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

8. PROCEDURE ADMINISTRATION

In accordance with procedure development and review protocol this procedure will be recorded as an authorised procedure approved by the Risk Management Working Group, at its meeting of the date shown on the front of this procedure document.

The procedure will be reviewed twelve (12) months from the date of the approval shown herein.

Notwithstanding the schedule review, should circumstance change significantly before the twelve (12) month review period, the policy will be immediately reviewed in order to maintain appropriate accuracy, relevance and authority.