STUDENT CYBER SAFETY PROCEDURE

Human Resources and Compliance
Version 3.0
Last Reviewed: 12 April 2018

1 Statement

St John's Anglican College is committed to the establishment and maintenance of a cyber-safe College environment and ensuring that exposure to inappropriate material or attention from other users is minimised.

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 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.

2 Scope

This procedure applies to the College Council members, employees and volunteers.

3 Principles

The responsibilities of 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 ICT 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 College places a high priority on providing Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation.
- 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 activities.

- The College has the dual responsibility to maximise the benefits of these technologies, while at the same time minimising and managing the risks.

4 Student Protection

The College supports the rights of children and young people and is committed to ensure the safety, welfare and wellbeing of students. The College is therefore committed to responding to allegations of student harm resulting from the conduct or actions of any person including that of employees. This commitment includes the provision of a safe and supportive living and learning environment for all students and requires all employees, volunteers and visitors to model and encourage behaviour that upholds the dignity and protection of students from harm.

5 Definitions

Cyberbullying:	is the use of technology for harassment, impersonation, denigration, trickery, exclusion and stalking
Social network sites:	such as Facebook, Instragram, YouTube, WhatsApp, Google Plus and Snapchat are services 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:	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 them in ANY way, including sexually, emotionally, psychologically or financially. Cyber predators know how to manipulate children, creating trust and friendship where none should exist.

6 Cyber Safety

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.*

6.1 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 pre-service teachers, 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.

6.2 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.

6.2.1 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.

6.2.2 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.

6.3 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 Privacy

Personal information is obtained, stored and released in accordance with the *Privacy Act 1988*. For further information please refer to the College's *Privacy Procedure*.

8 Accountabilities and Responsibilities

The table below outlines the accountabilities and responsibilities for governing and managing the College.	
College Council:	Is responsible for ensuring the proper and effective management and operation of the College. This includes defining and monitoring the strategic direction, developing and monitoring policies, monitoring the effectiveness of the College Council and College, and establishing control and accountability systems.

Principal:	Is responsible for the administration and implementation of the College's strategic direction, policies and procedures and control and accountability systems developed by the College Council. The Principal works closely with and is accountable to the College Council for leading the College to deliver high quality curriculum and educational outcomes, excellence in teaching and learning, a strong College community and driving market growth.
Manager Human Resources and Compliance:	Is responsible for ensuring the achievement of College strategic objectives through the development and application of best practice Human Resource Management principles and practices that comply with legislative requirements. The Manager Human Resources and Compliance works closely with and is accountable to the Principal for developing, implementing and evaluating an appropriate policy framework compliant with all statutory requirements.
Employees:	Are expected to abide by all College policies and procedures.

9 Related policies, procedures and other documents

9.1 Policies

Risk Management Policy

Student Protection in Anglican Schools Policy

Student Welfare Policy

9.2 Procedures

Behaviour Management Procedure

Critical Incident Management Procedure

Privacy Procedure

Student Anti Bullying Procedure

Student Pastoral Care Support Procedure

Student Protection in Anglican Schools Procedure

Student Self-Harm Procedure

9.3 Other documents

Australian Privacy Principles

Child and Youth Risk Management Strategy

College Vision, Mission and Values Statement

Faithfulness in Service

NetSafe Kit for Schools

Safeguarding Our Students, Student Protection Policy and Procedures Guide for Volunteers and Visitors to Anglican Schools

Staff Code of Conduct

Student Code of Conduct

Student Protection Resource Sheets

9.4 Legislation

Anti-Discrimination Act 1991

Child Protection Act 1999

Education (Accreditation of Non-State Schools) Act 2017

Education (Accreditation of Non-State Schools) Regulation 2017

Education Services for Overseas Students Act 2000

Education Services for Overseas Students Regulations 2001

Information Privacy Act 2009

National Code of Practice for Providers of Education and Training to Overseas Students

Privacy Act 1988

Right to Information Act 2009

Work Health and Safety Act 2011

Work Health and Safety Regulations 2011

Working with Children (Risk Management and Screening) Act 2000

Working with Children (Risk Management and Screening) Regulation 2011

9.5 Useful websites

NetAlert programme www.netalert.gov.au

Office of the eSafety Commissioner www.esafety.gov.au

10 Approval

This procedure was issued on 10 May 2018 under the authority of the Principal. This document represents the current policy of the College until it is revised or rescinded.

11 Managing this procedure

11.1 Review

This procedure is to be reviewed every two years or earlier if necessary. The Manager Human Resources and Compliance is responsible for reviewing or making approved modifications to the procedure and distributing.

11.2 Breach of Policy

All employees are expected to abide by College policies and procedures, failure to do so may lead to disciplinary action ranging from counselling to dismissal.

12 Document information

Version Control

Version	Date	Description	Author
3.0	12/04/2018	Procedure review	Manager HR and Compliance

13 Authorisation

Suzanne Bain
Principal
Date: 10 May 2018