Cyber Safety for Students Policy

1. Policy Statement

Kennedy Baptist College is committed to protecting students from harm by providing safe and secure online environments.

The College provides online services to students for curriculum-related activities and makes every reasonable effort to educate and protect students from exposure to inappropriate online material and activities.

Students are expected to access and use College devices and online products and services in accordance with the *Digital Citizenship Agreement* and *Student Code of Conduct*.

2. Scope

This policy applies to all students using approved devices, the College's computer networks and online services.

3. Rationale

School Registration Standard 5.1 requires the College to provide safe facilities which include guidelines and education for students, staff and parents about cyber safety and online security.

Student safety and wellbeing is an important prerequisite for effective learning in schools. Schools are expected to implement strategies in relation to cyber safety and cyber bullying.

The National Principles for Child Safe Organisations recognise the importance of safe online environments to promote the safety and wellbeing of all children and young people.

4. Definitions

Term	Definition
Cyberbullying	Cyberbullying is the use of technology to bully someone – to deliberately and repeatedly engage in hostile behaviour to hurt them socially, psychologically, or even physically. Cyberbullying can take place on social media, through online chat and messaging services, text messages, emails, on message boards and in online forums that allow people to publicly comment.
Cyber attack	An infiltration or blocking of an internet connected system or network with the intent to cause damage or disruption or gain unauthorised access to information.

Term	Definition
Internet	A global computer network which allows a range of information to be shared across the world. Also referred to as the "web" or "world wide web".
Network	A network is a group of computers that can communicate with one another.
Online	This can refer to a person using the internet (for example, "going online" or "searching online", or to a device or service that operates using internet access or capability (for example, "online banking").
Phishing	Phishing is the sending of fake emails to try to manipulate the receiver or obtain personal information from them. The emails often claim to be from a bank, online retailer, or credit card company. Recipients may be directed to what appears to be a genuine website for the organization or company, which encourages them to reveal financial details or other personal information.
Scams	Scams are dishonest schemes to take advantage of people to gain benefits such as money or access to personal details.
Spam	Unsolicited commercial electronic messages are known as spam. Under Australia's Spam Act 2003, spam includes emails, instant messaging, SMS and MMS of a commercial nature.

5. Introduction

Being safe online means to be safe and responsible online in accordance with the College's values of faith, integrity, boldness, growth, and service and with the support of parents/guardians.

6. Cyber Safety Strategies

6.1. The College has implemented policies to support students safety and wellbeing which clearly outline the values and expected standards of behaviour in all environments.

6.2. The ICT team identifies and manages online security risks to systems, equipment, and data and implements appropriate security controls to protect the delivery of critical infrastructure services.

6.3. All students are expected to adhere to the Digital Citizenship Agreement upon enrolment and students are asked to re-commit to the agreement each year. The agreement is an acceptable use agreement and

parents/guardians are also expected to support the Digital Citizenship Agreement.

6.4. The College will provide the College community with education regarding cyber safety on a regular basis and through the College Newsletter. Cyber safety will be regularly promoted at the College. Further education is covered in digital technologies classes.

7. How to be Safe Online

7.1. Students can always:

- Speak to a teacher they trust before going online.
- Ask any questions or get help if they're unsure what to do.
- Find out what websites or apps are safe to use.
- Find out what posts and photos are safe to share.

7.2. Students should never:

- Give out their personal information. Personal information includes their address, phone number or password.
- Let other people use their accounts.

7.3. If students meet people online and become friends:

- The student should be treated with respect.
- The student should feel comfortable with that person.

7.4. If students:

- Feel they are being bullied online such as receiving messages that are mean to them; or
- See something that makes them feel uncomfortable such as photos or videos that are violent or sexual, or messages that make them feel uncomfortable.

They should not respond to any messages and tell an adult they trust. The student may also block the person to stop them or report the person or message to the social media service (for example).

8. Reporting Concerns

The College will ensure the following process is implemented for students who report cyber safety incidents.

8.1. Identify the concerns – a cyber safety incident may include:

8.1.1. Cyberbullying.

8.1.2. Threats of violence or intimidation.

8.1.3. Image-based abuse and/or exploitation threat.

8.1.4. Exposure to graphic or pornographic images.

8.1.5. Viral threat.

8.1.6. Other online breaches of the Bullying Prevention Policy, Digital Citizenship Agreement, and/or the Student Code of Conduct.

8.1.7. Whether another student's actions have affected a student.

8.1.8. Whether a student's own actions have put themselves at risk of harm.

8.2. Ensure the students' safety by making further enquiries into the incident where possible.

8.3. Act on the information. The College's actions will depend on the incident, how much evidence can support the identification of the part(ies) involved and whether those part(ies) are students or not. If a criminal activity has occurred, the College will involve the appropriate authorities including Western Australian Police.

8.4. Provide support to any students and staff involved.

9. Resources

Guidelines and education for students, staff and parents about cyber safety and security include:

- Office of the eSafety Commissioner

  https://www.esafety.gov.au/

- ThinkUKnow

  https://www.thinkuknow.org.au/

Version control					
Version	Amendments	Date Reviewed	Endorsed by Board	Next Review	Author of version
1			20/05/2021	03/2023	
2	Amendment to title - Cyber Safety for Students. Amended 90% of policy.	01/08/2023	20/09/2023	03/2025	C Acciano
3	Amendment to policy statement.	07/05/2025	17/09/2025	03/2027	C Acciano