Computer Network, Online Users and Cybersafety Policy and Process

Operational

Category C

Version 2.0 Web

Contents

1 Purpose

The purpose of this policy is to ensure, as far as possible, the safety of the students when using the Covenant Christian School (the School) computer network. The policy also provides the obligations of the School to ensure that the network is secure so that students cannot access detrimental sites and that external hackers or predators are, as far as is reasonably possible, unable to access the School's computer network. The policy provides the requirements of students to use the computer network according to the rules and procedures for usage.

Covenant Christian School is committed to its Vision and Mission:

Vision:

In dependence on God's grace, Covenant Christian School will nurture and equip students with a heart to glorify God by serving Him and living according to His Word.

Mission:

Covenant Christian School is a safe, caring and loving community. In partnership with parents we cultivate Christian character in our students and equip them to serve God and contribute positively to society.

This will be achieved through a Christ-centred approach where the gospel is central. God's Word is applied to all areas of learning and experience. Students and staff are challenged, encouraged and supported to love learning and pursue excellence to the glory of God.

2 Organisational Scope

This policy is School-wide.

3 Policy Content and Guidelines

Internet access carries the potential to encounter information that may be controversial and/or inappropriate for students. Information on the Internet changes rapidly and it is not always possible to predict or control what students encounter. Since it is virtually impossible to control the Internet, it is the responsibility of the School and the family to teach students the skills needed to be responsible users. This document will define appropriate educational and ethical uses of the Internet, identify individual student responsibilities, and outline procedures for enforcing appropriate behavior on the Internet and handling violations.

4 Obligation on the School to Protect Children from Harm

The School has an obligation to maintain a safe physical and emotional environment for staff and students. This responsibility is increasingly being linked to the use of the Internet and Information, Communication and Learning Technologies (ICLT), and a number of related Cybersafety issues. The Internet and ICLT devices/equipment have the potential to bring great benefits to the teaching and learning programs, and to the effective operation of the School.

The School will respond to issues or incidents that have the potential to impact on the wellbeing of our students, including those reported through online services.

Some online activities are illegal and as such the School is required to report this to the appropriate authorities.

4.1 Internet Filtering

The School takes its obligation to protect students from online harm very seriously. It has extensive blocking / internet filtering applied by a network interface unit. In addition, Google's G Suite for Education (covenantsystems.org domain) is protected from external spam emails. However, full protection from inappropriate content can never by absolutely guaranteed.

4.2 Anti-bullying

The School places a high priority on providing Internet facilities and ICLT devices/equipment which will benefit student learning outcomes and the effective operation of the school. However, it recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the School and some privately owned by staff, students and other members of the School community), can also facilitate anti-social, inappropriate, and even illegal behaviour and activities. The School aims, therefore, to maximise the benefits of these technologies, while at the same time to minimise the dangers and manage the risks.

4.3 Right of Executive to monitor proper use

The School Executive has the right to question inappropriate Internet activities/materials, and may block access to an account at any time as deemed necessary. The School Executive also have the final say on what Internet activities/materials are inappropriate in accordance with the School's policies and philosophy.

4.4 The use of other technologies

The School has a strict policy on the use of mobile phones and other technologies during School hours. The rationale for this policy is based on several grounds, including:

- the potential for bullying of other students
- disruption in class
- the potential for some students to display such items as status symbols, and
- the staff duty of care towards each student.

The following apply to students:

- Students are not permitted to use their own mobile phones or electronic devices including, but not limited to, laptops, ipods, and iPads, within the School.
- All mobile phones and other electronic devices must be lodged with the designated School staff member at the commencement of each day and can be collected at the end of the day.
- Students using a mobile phone or electronic device without the express permission of the School Executive or delegated authority will have it confiscated until it is collected from the office by one of their parents.

5 Obligations on Students to Comply with Relevant Sections of this Policy

Students must comply with the relevant sections of this policy in relations to the use of the School's network. To obtain permission to use the network, students must read and sign the User Agreement at Appendix A.

5.1 Expectations and Conditions of Proper Use

1. The School's network shall be used only for educational purposes consistent with the School's ethos and beliefs.
2. Users must only use those programs in class that a teacher has approved for the lesson.
3. Users must be polite and use appropriate language in all interactions using School computing resources.
4. Users must respect School policies and behaviour standards.
5. For users obtaining a password, passwords may be changed at any time by the system administrator.
6. Users should not have an expectation of privacy for any activities/materials, including, but not limited to, email on the School's Internet domain (covenantsystems.org).
7. Users must respect all copyright laws. Questions regarding use of copyright materials will be directed to the system administrator. Plagiarism is prohibited and is defined as taking the idea or writing of others and presenting them as one's own.
8. Users must respect equipment, system performance, resources and use of time on the network.
9. Users must respect the privacy of others.
10. Network users identifying a security problem on the School's system must notify the teacher or system administrator immediately. Explain the issue but do not demonstrate the problem.
11. Any items produced by students will not be posted on the publicly accessible Internet without parent/guardian permission.
12. Any network user identified as violating School computer use guidelines may be denied access to the School's network.
13. The School reserves the right to change, restrict, limit or deny the use of computing resources and access to users when deemed necessary.

5.2 Prohibition

1. Students must not share passwords.
2. No unapproved software may be loaded onto the School's computers and/or network.
3. Attempts by a student to log on to the School's system in the name of another student or teacher, with or without that person's password, is prohibited.
4. Interference with another person's computer or their files is prohibited.
5. Use of computer access to data and access to secure areas of the School's network, other than for approved educational purposes is prohibited.
6. Vandalism of the School's computing resources may result in cancellation of system use privileges in addition to other disciplinary measures.
7. A user shall not access or upload material that is profane or pornographic or that advocates violence toward other people or any material contrary to the School's Christian ethos.
8. Any use of the School's technology resources for illegal activities is strictly prohibited. The School will cooperate fully with territory or federal authorities in any investigation related to any illegal activities conducted using the School's resources. Where relevant, a user may face charges by the police.

9. No student is permitted to run unauthorised software from a device or to copy music/videos/games or unauthorised software to any part of the School's network.

5.3 Violations of this Policy

Any student found in violation of this policy will be subject to appropriate action including, but not limited to:

- temporary suspension of their School computer access, and/or
- other appropriate disciplinary action in accord with the policies and procedures of the School.

5.4 Access Requirement

Students will have no access to the School's computer resources until the Computer Network, Online User and Cybersafety Policy Signature Form is signed and returned.

6 Legislative Compliance

Crimes Act 1900 (ACT)
Disability Discrimination Act 1992 (Cth)
Disability Standards for Education 2005 (Cth)
Discrimination Act 1991 (ACT)
Human Rights Act 2004 (ACT)
Human Rights and Equal Opportunity Commission Act 1986 (Cth)
Information Privacy Act 2014 (ACT)
Racial Discrimination Act 1975 (Cth)
Sex Discrimination Act 1984 (Cth)

7 References

eSafety Commissioner link

8 Appendices

Appendix A: Computer Network, Online Users and Cybersafety Signature Form

9 Approval Agency

The Principal

10 Policy Sponsor

The Principal

11 Contact Person

The following person may be approached on a routine basis in relation to this policy:

The Business Manager
[Ext: 103]

12 Appendix A

COVENANT CHRISTIAN SCHOOL

COMPUTER NETWORK, ONLINE USER AND CYBERSAFETY POLICY SIGNATURE FORM

Student Agreement

I have read the requirements outlined in Section 5 of the **Computer Network, Online Users and Cybersafety Policy** and agree to abide by the rules and their intent to maintain a safe, inclusive and supportive learning environment, and I understand that there are consequences for violating the expectations for appropriate use.

I understand that when I use the computing resources of Covenant Christian School, I must not store any private information. The system administrator may monitor my files, as well as my Internet access as part of his/her duties of supervision.

Student's Name: _____ Year level: _____

Signed when read: _____(Student)

Date: _____

Parent/Guardian Agreement

I have read the requirements outlined in the **Computer and Network User Policy** and agree to abide by the rules and their intent, and I understand that there are consequences for violating the conditions set.

Parent / Guardian Name: _____

Signed: _____ (Parent/Guardian)

Date: _____