CROW'S NEST STATE SCHOOL

ICT PRIVACY POLICY

Crow's Nest State School protects and caters for the privacy of students who use ICT devices. In line with the Queensland Government Information Privacy Act 2009 (Qld), the following policy outlines the precautions and expectations for CNSS staff in protecting the privacy of student ICT usage, BYOD usage and Internet usage.

Table of Contents

Overview

Introduction

Crow's Nest State School has adopted the endorsed guidelines of Queensland's Department of Education to allow students to bring personal devices to school to facilitate the use of technology integration into the classroom using multiple strategies.

This document outlines how CNSS utilises all ICT data that is captured from student network usage, including BYO usage. This document also outlines the precautions and expectations CNSS staff will undertake to ensure student privacy and personal information is safe.

Monitoring Student Usage

Device Monitoring

School owned student devices will be monitored on school campus. Classroom management software solutions can include, but are not limited to products such as 'AB Tutor'. All students who utilise school owned devices and do not participate in the schools BYO program will be subject to device usage and monitoring as agreed upon by the '*ICT Network Usage Agreement*'.

Student owned computers will not have this monitoring software solution installed and will not be subject to application and usage monitoring outside the scope of the '*ICT Network Usage Agreement*'.

Privacy protections

CNSS guarantees students the following privacy protections when using classroom management software; therefore, **CNSS will not save/log and record** any:

- personal usage of devices, including access to personal files, information, games, movies, music, passwords and personal account access
- screen captures of student devices
- keyboard keystrokes

Additionally, CNSS guarantees that teachers will not manipulate operating systems, install software, access student files or control devices without student consent.

The use of **device monitoring will only be used for**:

- Visual monitoring of device usage in the classroom for lesson task management
- Locking of devices when students are not completing class approved activities and are being continually distracted or distracting to themselves and peers
- Limiting software access during lessons to ensure appropriate task completion
- Taking control of the student's machine, with student consent, to assist students
- Sharing student screens for educational purposes, with student consent

If inappropriate use of a personal device is identified, as agreed upon by the '*BYOD Policy*' and school '*ICT Network Usage Agreement*', the matter will be referred to the Head of Department or Principal as a course of action outlined by CNSS '*Student Code of Conduct'* policy.

Pirated/Illegal/Explicit materials

If a staff member observes the use, viewing or distribution of pirated, illegal or explicit digital materials, the incident will be referred appropriately to the Head of Department or Principal as a course of action outlined by CNSS '*Student Code of Conduct'* policy and as agreed upon by the '*BYOD Policy*'.

Staff usage of device monitoring

Approved monitoring of school owned devices will be delegated by the Principal. Approved delegates will have appropriate training and adhere to the Privacy Policy guidelines as identified in this document.

Internet Monitoring

All student access to the internet is filtered by our department's firewall and websites deemed harmful and non-educational are blocked within the school network.

Privacy protections

Only approved delegates, as identified by the Principal, have access to student browsing history through the department's Managed Information Services portal (MIS). MIS automatically logs all student access requests to the internet while using school owned network infrastructure. Once a student is off-campus, no internet logging occurs.

No unauthorised access to this information will occur. Access to school internet browsing history via department firewall logging will be available at the discretion of Head of Department and Principal for investigations into breaches of misuse and defined by the '*BYOD Policy*' and school '*ICT Network Usage Agreement*'. Any identified usage that is deemed inappropriate will be subject to our CNSS '*Student Code of Conduct'* policy.

Email Monitoring

All EQ emails transmitted within the department are monitored and filtered for keywords that may be inappropriate or harmful. Any email that is deemed inappropriate by keyword/phrase filtering is intercepted into a quarantine mailbox and may result in a school-based consequence. Any identified usage that is deemed inappropriate will be subject to our '*Student Code of Conduct'* policy.

Privacy protections

Only approved delegates, as identified by the Principal, have access to the email quarantine mailbox which is managed through the department's Managed Information Services portal (MIS). MIS automatically filters all student emails for keywords and phrases that can be identified as harmful. This includes, but not limited to, threats, bullying, swearing, inappropriate attachments etc. Once a student is off-campus, email filtering continues, so long as that student is using their eq.edu.au email alias.

No unauthorised access to this information will occur. Access to quarantined emails will be available at the discretion of the Head of Department and Principal for investigations into breaches of misuse and defined by the '*BYOD Policy*' and school '*ICT network Usage Agreement*'. Any identified usage that is deemed inappropriate will be subject to our '*Student Code of Conduct'* policy.

Third-party Websites

The use of web based educational resources has risen steadily over the last decade and increasingly web based resources are being used by teachers across Queensland to improve student learning outcomes.

Crow's Nest State School teachers make decisions about the best technology to meet the needs of our students. Sometimes it is beneficial for students to utilise services provided by third party web-based providers.

For students to use some third party services the teacher will need to register them as users. Registering with these providers requires student personal information to be disclosed to the provider of the service. In the case of many of the websites CNSS will utilise, they are private companies that host their platform data services in Australia. In instances where websites that CNSS wishes to utilise for educational purposes are hosted outside of Australia, this means that data that is entered to register students will be stored on servers that are not based in Australia and therefore are not bound by Queensland's privacy laws. Registration may include disclosing the following information about your student:

- Student name
- Student EQ ID
- Age
- Year group
- Class teacher; and
- Student email

A comprehensive list of websites is provided annually and during enrolment in the '*Third-party Websites Consent Form*'.

Privacy protections

In all cases, when a website is identified for educational purposes that requires student/user accounts to be generated, the Head of Department and teachers must investigate the appropriateness of the website in question and amount of information required to generate the accounts.

A website risk assessment is conducted to identify what information is being supplied to the third-party provider and whether that information will be appropriately used and is safe. Many of these websites are reviewed through the Department of Education Website Risk Review registrar.

CNSS will responsibly manage which websites have access to student information and in all cases, limit the amount of personally identifiable information made available.