OKAIHAU COLLEGE POLICY: CYBER SAFETY

Introduction

This policy is designed to meet the school's statutory obligations to maintain a safe learning environment and to consult with the community. As well, the board is aware of its responsibilities to be a good employer. The overall goal is to maximise the educational benefits of communication technologies while minimising the risks.

Use of the Internet and other communications technologies at Okaihau College is to be limited to educational and personal usage appropriate in the school environment. Appropriate use also includes staff professional development.

'Other communication technologies' includes but is not limited to computers (including laptops), storage devices, video/digital cameras, video/audio/ players/receivers, gaming consoles and mobile phone and technologies associated with internet use e.g. web cam. Included, too, are similar technologies still to be developed that allow the communication of one person to another using any communication device or medium.

The communication technologies at Okaihau College are available to staff and students under certain conditions, as outlined in the signed Use Agreement. The school will make basic training available for staff using these technologies. Associated professional development needs will be considered.

Appropriate cyber safety measures will be put in place and enforced by the school. In order to ensure the safety of the school learning environment, action should be taken if these safety regulations are breached by students or staff.

This Cyber Safety Policy applies to all employees of the Board (i.e. teaching, support and ancillary staff) and to all students. It also applies to teacher and other professional trainees assigned to the school from time to time e.g. long term Relief Teachers. Any Board member requiring access to the school's communication technologies are to required to following the same guidelines and responsibilities as other staff.

The board recognises the need for on-going funding for cybersafety practices through inclusion in the annual budget, the review of the school's annual and strategic plan, the deployment of staff, professional development and training, implications for the design and delivery of the curriculum, the need for relevant education about cybersafety for the school community, disciplinary responses to breaches of cybersafety, the availability of appropriate pastoral support and potential employment issues.

The Principal or delegate will report regularly to the Board on the school's implementation of this Board Policy.

Guidelines

1. All students must read and sign a Cyber Safety Use Agreement outlining the regulations and conditions under which computers and communication technologies

may be used while at school or in any way which affects the safety of the school learning environment. The agreement must also be signed by a parent/caregiver.

2. Students will be supervised while using school facilities; the degree and type of that supervision may vary, dependent on the type of technology concerned, where the equipment is physically situated and whether or not the activity is occurring in the classroom.

3. All staff must sign a Cyber Safety Use Agreement which includes details of their professional responsibilities and the limits to their own use of the Internet.

4. Educational material on cyber safety will be provided by management to staff and students and to parents/caregivers. As well, additional safety education will be delivered, where relevant, through teaching programmes.

5. Basic training for staff will be made available by management, as will appropriate professional development.

6. The necessary procedures will be put into place by the school to address cyber safety issues in all venues where the Internet and other communication technologies are accessed by staff or students.

7. The school will provide an effective electronic security system, which is financially practicable. The school will continue to refine methods to improve cyber safety.

8. The Principal will be responsible for the establishment and maintenance of a cyber safety programme in the school. (The Principal may well delegate that responsibility to a member of the Senior Management Team.)

9. The Board supports the right of the school to check communication technology related work or data of staff or students at any time, and to carry out a comprehensive investigation of any breaches of the school's cyber safety policies. Such breaches will be taken seriously and be dealt with through the school's disciplinary and support systems.
In such incidents, there will be special attention paid to the need for specific procedures as regards the gathering of evidence. If illegal material or activities are suspected, the matter will be reported to the Police or the Department of Internal Affairs Censorship Compliance.

9. 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 Privacy Act 1993.

10. The school will consult with the wider school community and provide opportunities to learn about cyber safety issues e.g. through Parent Information Evenings.