Coastal Taranaki School Cyber Safety Policy

Coastal Taranaki School has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. Coastal Taranaki School will develop and maintain rigorous and effective cyber safety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.
Associated issues the school will address include:
· funding for cyber safety practices will be budgeted for as applicable.
· 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 cyber safety for the school community
· disciplinary responses appropriate to breaches of cyber safety
· the availability of appropriate pastoral support
· potential employment issues.

To develop a cyber safe school environment, the board will delegate to the principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programmes. All Board members will be included under the parameters of this procedure.

Guidelines for Coastal Taranaki School's Cyber safety Practices

1. The school's cyber safety practices are to be based on current best practice.
2. Cyber safety agreements for any members of the school community using school equipment will be signed. This includes off-site access to the school network from school or privately-owned/leased equipment.
3. Coastal Taranaki School cyber safety agreement covers all members of the school community.
4. The user agreements are also an educative tool and should be used as a resource for the professional development of staff and learning of students. All use of CTS ICT facilities will be appropriate to the school environment as defined in use agreements.
5. Signed use agreements will be filed in student and staff personnel files.
6. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times. This includes all digital devices.
7. The school has the right to audit, at any time, any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity. 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.
8. 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 school's cyber safety practices. In serious incidents, advice will be sought from an appropriate source, such NetSafe, the New Zealand School Trustees Association 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.

12. CYBER SAFETY

Important terms used in this document:
(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies.
(b) **'Cybersafety'** refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones
(c) **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below
(d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/ receivers (such as portable CD and DVD players),Gaming Consoles, and any other, similar, technologies as they come into use.
Important terms used in this document:
(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies.
(b) **'Cybersafety'** refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones
(c) **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below
(d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/ receivers (such as portable CD and DVD players),Gaming Consoles, and any other, similar, technologies as they come into use.