BHBI School	Policy / Procedure manual
CYBER SAFETY	NAG 1

Purpose
The purpose of this procedure is to ensure that Blockhouse Bay Intermediate School (BBI) meets its statutory obligations to maintain a safe learning environment and to maximise the educational benefits of communication technologies while minimizing the risks.

Definitions
'Other Communication Technologies (OCT)' includes mobile phones, digital cameras, IT devices, webcams, and any other internet associated technologies including those currently being developed.

Principles
The following principles guide cybersafety at BBI:

1. The Cybersafety procedure applies to all employees of the BOT, BOT members, relief teachers, teacher/other professional trainers/trainees, all students and others requiring logins.
2. Use of the internet and OCT at all times are to be limited to educational and personal usage (including staff professional development) appropriate in the school environment.
3. Only individuals who have read and signed the Cybersafety Use Agreement are able to use BBI's OCT.
4. Appropriate cybersafety measures will be established and enforced to ensure safety of BBI's learning environment. Any breach of cybersafety regulations may result in disciplinary action. BBI will continue to refine methods to improve cybersafety.

Processes

1. The Principal or their delegate will report regularly on any breaches to the BBI BOT on implementation of this procedure.
2. The Principal will appoint a BBI Cybersafety Officer (CO), who will be the main contact point for all OCT issues/incidents and will report to the Principal.
3. The CO will advise the Principal on the establishment and maintenance of BBI's cybersafety programme including appropriate policies, procedures and User Agreements, an effective electronic security system, and a comprehensive BBI cybersafety education programme.
4. Teachers will ensure students are familiar with, have read and signed the Cybersafety Use Agreement outlining regulations and conditions under which computers and OCT may be used while at BBI or in any way which affects the safety of BBI's learning environment. All Cybersafety Use Agreements signed by students must also be signed by a parent/caregiver.
5. A system will be established whereby classroom teachers can readily access the names of any students who do not have a signed Use Agreement on file as they are not permitted to access relevant BBI technologies.
6. Students will be supervised while using BBI facilities; the degree and type of supervision may vary dependent on the type of technology concerned, where equipment is physical situated, and whether or not the activity is occurring in the classroom.

7. Cybersafety educational material will be provided by management to staff and delivered, where relevant, through the teaching programme.
8. Necessary procedures will be implemented to address cybersafety issues in all venues where the internet and other OCTs are accessed by staff or students.
9. A financially practicable effective electronic security system will be provided.
10. BBI BOT supports BBI's right to check OCT-related work/data of staff/students at any time, and to carry out comprehensive investigations of any breaches to the cybersafety policies.
11. At the commencement of employment, all BOT employees must read and sign the Cybersafety Use Agreement.
12. For staff working with students, this agreement includes details of their responsibilities to actively supervise/monitor student internet use to report any breaches of the procedure to the CO. This agreement also informs staff of the limits to their own use of the internet, and of the privacy issues associated with confidential information on BBI's network.
13. Staff are responsible for internet-accessible computers in their care and for relevant cybersafety procedures to cover their particular situation.

Breaches

1. Any breaches of cybersafety regulations should reported to the CO and the Principal or other member of the Senior Management Team and will be dealt with in accordance with BBI's usual disciplinary procedures.
2. If a serious breach has occurred, vital preservation of evidentiary trail, appropriate documentation and external consultation should occur as well as appropriate legal advice.
3. If any illegal/objectionable material/activities are suspected, the Police, the Department of Internal Affairs Censorship Compliance or any other appropriate outside agency may be notified.
4. Staff should be aware of their responsibility to maintain cybersafety in their classroom including reminding students of cybersafety rules before starting any unit of work involving use of the internet or other OCT, actively supervising student use and checking that the siting of internet-accessible computers takes into account safety issues.
5. Teachers are to assist students develop the skill base to effectively use the internet as a learning tool.