ICT Acceptable Use Policy and Acknowledgement

Overview

The School has invested a significant amount of monetary and other resources in information technology infrastructure to further the pedagogical and other aims of the School. This document outlines some of the issues and responsibilities which you as a user must be aware of, and accept, in your use of these facilities. Each of us is personally responsible for ensuring these investments are protected and shared at all times.

Access

You will be provided with access to the internet, applications and to appropriate areas of the School ICT network.

Access to the network by computers not owned by the School

You may access the network using a computer that is not owned by the School, provided you adhere to School polices. This includes laptops, and computers located at home but connected to the School network. Limited support will be provided to enable you to use these personal resources on the School network, although final responsibility and maintenance of your computer rests solely with you.

Training and Support

Appropriate instruction in the use of the School network, workstations, and software will be made available to you.

Data Storage

You may store data files on the network server. We encourage the responsible use of space on the server, and the removal/archive of older material. Personal files should not be stored on the School network.

Privacy

No guarantees can be given for the privacy of files. However, system administrators will not examine the contents of personal documents without the individual's knowledge, except in system emergencies or under unusual circumstances such as a breach of this policy.

Use of Printers and Peripherals

You will be able to use School facilities for work related to the School, including printers, scanners and digital cameras.

Personal Usage

Incidental personal use of School resources is acceptable as long as it does not interfere with the use of our facilities for their intended purpose, and as long as it does not interfere with your duties. Note that personal computers connected to the School network will be required to meet School standards of security and virus protection.

Adherence to School Policies

All appropriate policies of the School, including the Copyright, Plagiarism, and Harassment Polices, apply to you while using our facilities.

Data Storage

While every effort will be made to preserve any data, you place on the network, it is up to you to safeguard your information, through "back-ups" on portable storage devices etc (flash drive, memory stick).

User Identity and Logon

It is critically important that you logon and logoff with your own BMGS username and password. This ensures the privacy of your files on the server and safeguards these files from other users.

Exposure to External Information Sources

The School is not responsible for Internet users and/or content that originates from outside the School.

Examples of Prohibited Uses

The following are considered inappropriate, and may result in consequences, as outlined in the policy. Users are expected to use their own judgement, as the following are representative examples only and do comprise a comprehensive list of unacceptable uses:

1. Impersonation of another user, individual, organisation for any reason (this includes representing your ability to speak of the School);
2. Unauthorised viewing of/or entry into a file, directory, database, server, computer system or network to which you do not already have legitimate permission to use/access;
3. Unauthorised attempted or actual destruction or alteration of data or information;
4. Attempting in any way to interfere with anyone else's use of their computer, network etc; this includes spamming (sending large volumes of email to a particular user), flooding a link with extraneous information, etc and virus propagation;
5. Sending or replicating chain letters, virus "alerts", or participating in pyramid schemes using the School computing facilities for any commercial purpose whatsoever;
6. View or transmit by any means information that might be reasonably expected to be perceived by the recipient(s) as being threatening, harassing, violent, offensive, pornographic, racist, defamatory, sexist etc.
7. Inappropriate disclosure, sharing, disseminating or disposing of private information as outlined in the Privacy Act 1988.

Installing and Downloading Software

Users should consult with the ICT Manager if they wish to make significant changes to a School-owned computer system.

Copyright

Users must respect the legal protection provided by copyright laws for computer programs and data compilations and for all other works (literacy, dramatic, artistic or musical).

Security of School Computers

If you become aware of any inappropriate or suspicious activity which may compromise School data, computers or networks, regardless of the origin, please report it at once to the ICT Manager. The School depends upon all of us to safeguard our computer systems and confidential data.

Consequences

The School is legally obliged to ensure prohibited activities as outlined above do not take place by persons accessing the internet from computers connected to the School network. Evidence of such activities may result in:

1. Suspension or withdrawal of computer services
2. Internal disciplinary action
3. Legal action by the authorities in Australian or other jurisdictions

Declaration of Acknowledgement

Please sign to indicate that you have read and understood the policy.

Name

Signature

Date Submitted ☐☐/☐☐/☐☐☐☐