INFORMATION COMMUNICATIONS TECHNOLOGY POLICY - STAFF AND STUDENTS

Educational Rationale

As we educate our students for a rapidly changing world, we believe that it is of vital importance that we provide our students with a wide range of learning experiences, utilising Information and Communication Technologies constructively and responsibly to help prepare them for life in the 21st Century.

The Internet is a global network, linking computers at universities, schools, government departments, businesses and homes. On the Internet, one can access information and communicate with people all over the world through web sites, discussion forums, as well as through electronic mail.

Use of the Internet will provide many direct and indirect benefits to our students. These include:

- access to vast libraries of information from sources throughout the world
- the ability to interact and collaborate with other students and knowledgeable adults
- the acquisition of knowledge, abilities and skills that will be useful throughout their lives
- the opportunity to publish their own material to a wide audience
- As a communication medium, the Internet's potential is boundless. However, although the Internet is of significant educational value, care needs to be taken with its use in order to exploit efficiently, effectively and appropriately this potential.

How Students use the Internet at the College

The use of the Internet at GBC will be developed as part of each student's learning program.
Students will have access to the World Wide Web and Email through the College's networked computers. Although each student's use of the Internet will be derived from the educational context, it is possible that she may come across material on the Internet that is not in accord with the College's or your family's values. As a school we are addressing appropriate Internet access with our students and we would encourage parents to discuss these matters with each student in the light of your own family's values.

During class time, teachers are responsible for student use of the Internet. For use outside class time a student can also access the Internet for personal research and communication only if they have express permission from their teacher.

Student General Responsibilities

As with all resources provided by the College, the College's Internet connection is for educational purposes. The most important prerequisite for Internet use is that the student takes full responsibility for her own actions and their effect on others. It is the student's responsibility to:

- not post messages and attribute them to other users
- not to use email to copy information that is personally abusive to the recipient or any other person
- not interfere with, harm or destroy the computer work of any person
- not break copyright law by copying and/or redistributing another's work
- not copy the ideas of others and present them as her own (plagiarism)
- refrain from excessive printing
- not reveal personal information including names, addresses and telephone numbers of self or others
- acknowledge appropriately downloaded material used in preparing work
- Not tell any other individual their network password. It must be remembered that all individuals are responsible for their own account, and no individual shall use another's account.

** Failure to observe these requirements will result in loss of computer privileges and if offences are repeated, may result in the student being withdrawn from the College.

Implementation

1) The College actively supports access by students to the widest variety of information resources available, accompanied by the development of the skills necessary to filter, analyse, interpret and evaluate information encountered.

2) All students and staff will have censorship filtered internet and email access. All students and staff will have their own password protected internet account and log on. Such access is a privilege that infers responsibility, and not simply a right to be expected.

3) An ICT Coordinator will be appointed, who will liaise with staff and the technical support technician to manage all email access, maintenance of the school's web site, web filters, and all other issues related to internet access by students.

4) Student behaviour when using school computers and networks, when using the internet and e-mail, and when engaging in any activity with College computers must be consistent with the College's ICT Policy and Student Discipline Policy.

5) The College undertakes to ensure that information published on the Internet by students or the school is of a high standard, and meets legal requirements and standards of general practice within the community in relation to copyright, safety and decency.

6) All email accounts will be password protected and users will be responsible for clearing their mailboxes regularly.

7) All students shall be responsible for notifying their teacher of any inappropriate material so that access can be blocked.

8) All staff shall be responsible for notifying the ICT Coordinator of any inappropriate material so that access can be blocked.

9) Privacy of students, parents, staff and other users must be recognised and respected at all times. When identifying students or when student's identify themselves only the first name and last initial will be used.

10) Consequences of publishing, accessing or failing to notify the Coordinator of inappropriate material shall include the removal of access rights.

11) Staff are expected to utilise and integrate technologies, including on-line learning opportunities, into their programs for all students.

12) Teachers shall be responsible for making sure all work is screened for accuracy, appropriateness, grammar, spelling prior to publishing.

13) Signed parent and student consent (in Student Discipline Policy) is required to be completed in order to gain access to the internet.

14) The College aims to provide appropriate professional development and support for all staff.

UNDESIRABLE CONTENT – GUIDELINES AND PROCEDURES

As a member of the Geelong Baptist College community and a user of IT resources, it is important that you are shielded from the 'undesirable electronic content' of computer communications, such as pornography or related matters.

For this reason we have created the following guidelines and procedures for use by staff and students.

Undesirable Material – Definitions

Undesirable material comes in many forms; key to this definition is the purpose of the material:

- Is it for educational purposes?
- Does the material reflect the ethos and core values of the College?
- If the material does not comply, then the procedures as outlined below will apply.
- Students and staff are responsible for material in their own College folder. Regular checks should be made and passwords can be changed through the ICT Coordinator.

What Constitutes Undesirable Material?

Staff that may be involved in determining compliance: ICT Coordinator, Discipline Coordinator, Head of Secondary or Primary Coordinator. If there is uncertainty, then it will be referred to the Principal. A School Chaplain may be required to act as a consultant on some matters. In the case of issues relating to misuse by staff members, the matter will be referred directly to the Principal.

As a guide, the following points may arise and need to be dealt with under the policy. Please note that this list is not definitive.

- Undesirable posters or icons as screen savers, pointers or in folders etc.
- Topless or nude males or females.
- College students (or other students) in compromising positions.
- Sexually explicit material in any format, including animation, video, self produced cartoons, photos etc.
- Undesirable naming of files, folders or persons.
- Unacceptable MSN dialogue, chat or email.
- Material that could be offensive to anyone. This includes information that is racist, sexist, pornographic, irreligious or contains abusive language
- Any material that is or could be perceived as dangerous, illegal, containing violence or the like.

Procedures

The ICT Coordinator will conduct random searches and will follow the protocols as established. There is no requirement for any other staff member to specifically search for undesirable electronic content on computers.

All staff members: if it is suspected that undesirable content exists, or upon discovery of any undesirable content, it is to be reported to the ICT Coordinator for processing purposes.

ICT Staff – on discovering undesirable material: Report details to Discipline Coordinator or Principal.

If the offending material is on the network, then a copy of the folder will be taken and deposited at the Front Office for investigation by the Discipline Coordinator or the Principal and the material subsequently deleted.

The steps that may follow include:

- Suspension and parent involvement - the first action in most instances.
- Low level discussion with Director of IT or the House Coordinator.
- Withdrawal of enrolment.
- In the event of severe breeches to the guidelines, reporting to authorities will occur.

ICT POLICY – ACCEPTABLE USE

This policy applies to the users of the College network, email, internet, intranet and other electronic equipment. This includes but is not limited to all students, staff, contractors, casuals, temporaries and volunteers.

1. ACCEPTABLE   USAGE

1) The behaviour of each individual using the College network must be appropriate at all times and must abide by the College's policies. Each individual using the College network agrees that they are solely responsible for their actions, or the actions of others, for all material accessed and all actions undertaken whilst under their account on the network.
2) The network is for the purpose of school related study and not for personal needs. This includes unauthorised use of another person's tablet/notebook computer or accessories. Games or music are not to be played during school hours without permission of staff.

2. INTERNET ACCESS

1) The individual using the College internet connection is responsible for all material accessed under their account.
2) The internet connection is to be used for school research, assignments and other school related activities only. Not for: games, music, movies and all other unrelated school material including the use of chat and/or recreational programs.
3) Students are advised not to publish personal or defamatory information on to personal website or public forums. Doing so may endanger their personal safety or result in legal action.

3. EMAIL USAGE

1) The College provides an email account for all users. The email system provided is to be the only one used on the school network.
2) The email tool is to be used for the purpose of electronic communication between two parties. It is not to be used for spam, annoying, harassing or abusive emails, this includes 'chain' or 'forward (fwd)' emails. Email is considered harassment if it offends the receiving party in any way.
3) The individual is responsible for all emails sent and received on their email account.
4) No individual shall post their student email address on a web page external to the College.
5) No individual shall store, send or knowingly receive any pornographic, or other sexually explicit material.
6) No individual shall knowingly send or receive any email containing any material that could be perceived as dangerous, illegal, containing violence or the like.
7) No individual shall send unauthorised broadcast messages.
8) It is necessary to delete old emails and clear the 'sent items' and 'deleted items' folders on a regular basis, to ensure sufficient free space to fully utilise email functions.

4. USE OF COMPUTER LABORATORIES / RESOURCES

1) No individual shall eat or drink in a computer lab. Person(s) found breaching this rule may have their account(s) disabled for a time.
2) No individual shall change system settings, including screen savers and desktop wallpapers.
3) No individual shall intentionally damage or abuse computer equipment. Persons found intentionally damaging computer equipment will have their account(s) disabled for a time, as determined by a Coordinator or Head of School, and other consequences as may be deemed necessary.
4) No student shall be in a computer lab without being under the supervision of a staff member.
5) It is the individual's responsibility to backup their own data on a periodic basis.
6) No individual shall download, use or store any hacking software on the school network, or on their notebook computer/tablet.

5. REVIEW AND MONITORING OF NETWORK USERS

1) Upon logging onto the network, the individual understands that his or her actions may be monitored at any time.
2) Monitoring of user accounts may include tracking of web pages visited, all material downloaded from the internet and scanning of files saved on the individuals network drive.
3) Emails sent and received may be monitored and viewed.
4) USB keys and other storage media are governed by this Policy, in that they must not contain material deemed to be offensive, copyright etc. These may also be subject to random screening.

6. ELECTRONIC HARASSMENT

1) GBC has an anti harassment policy. This policy endeavours to create a climate of acceptance, care and support for each member of the GBC community. GBC will not tolerate the oppression of one member by another. Everyone has the right to feel safe from any form of harassment, including electronic harassment.
2) If a particular behaviour embarrasses, upsets or hurts another individual, then it can be classified as harassment.
3) No individual shall harass any other individual through the use of email or other electronic means.

7. VIRUS AND VIRUS HOAXES

1) The purpose of a virus is to disrupt a computer and/or network.
2) No individual shall knowingly download, activate, use or store any virus type of program on the College network. This includes any type of worm, virus or Trojan horse.
3) GBC uses virus scanning and spy ware prevention technology. Individual users are not permitted to load alternative software or attempt to disable anything provided by the College in respect of this.

8. THE INTERNET AND COPYRIGHT

1) Australian copyright law does not allow for copyright material to be copied to the network, a notebook, hard drive or to other media such as CDs, DVDs or iPODs that you may have purchased.
2) Copyright infringement by students and staff will be treated as misconduct.
4) The College provides students and staff with access to computer systems and facilities for academic purposes. Persons who are found to be using the College's systems to engage in conduct which infringes copyright, including uploading and downloading files without the permission of the owner of copyright, are exposing themselves and the College to legal action and will be subject to disciplinary action.
5) The web is NOT a copyright-free zone. DO NOT assume that you are entitled to download everything you can access on the web. Some material may be on the web without the copyright owner's permission.
6) DO NOT assume that because you can locate music (or other) files through applications such as peer-to-peer clients like Limewire or Torrent networks and so on, that you can download, copy or transfer them, even for personal use. Be aware that the download and or installation of any of these programs on school owned computers is not allowed.
7) DO NOT, without the permission of the owner of copyright,
    a. post music or other files to the College websites
    b. transfer music or other files to friends and family via the College email
    c. burn music or other files to CDs.
8) DO NOT use College equipment, student tablet/notebook computers or the computer networks to download, redistribute or copy unauthorised files.
9) There are some websites which offer, with the copyright owner's permission, MP3 files or other music formats for free download. The College's computers and network should NOT be used for this purpose. If you want to download or transfer music for any non-academic purpose, this should be done privately, and not on a College-owned computer or through the College's computer network.