Acceptable Usage of Technology Policy at GCCC

Purpose

The purpose of this policy is to set out the acceptable usage parameters of technology in the College. The computers and computer network at Glasshouse Country Christian College together with access to the internet and email are provided for educational and professional purposes. The use of these facilities should therefore be consistent with that purpose, as detailed in this document.

Scope

College employees and students must adhere to all elements of this policy.

Principles

The principles of behaviour relating to the use of school resources include: respect for the law; respect for other people; and respect of the Glasshouse Country Christian College’s mission and values. The principles of conduct also assume integrity, diligence, economy and efficiency from the users.

Classroom Requirements

Teaching staff have a responsibility to:

- Ensure that students have clearly defined tasks for using the on-line services and resources,
- Provide appropriate levels of supervision,
- Educate students about intellectual property and copyright laws,
- Provide students with an ethical understanding of the issues regarding plagiarism, and
- Educate students about the information handling skills of on-line research, including evaluating, verifying and citing the on-line sources of their information,
- Educate students in locating suitable resources available through catalogues, directories and teacher developed resources lists, and also when to use search engines.
- Maintain confidentiality of personal username and password
- Only use the computer under your personal username and password

Students have a responsibility to:

- Maintain confidentiality of personal username and password
- Comply with instructions of teacher,
- Conform to acceptable school behaviour, conduct and standards,
- Refrain from bringing music, mp3 files and any other non-school related digital material and devices
- Respect the equipment and not cause deliberate damage or modification
- Respect the network security of the College and refrain from attempting to ‘hack’ the network or gain access to the network via someone else’s login and username.
- Ensure that, when required, electronic media is virus checked prior to reading or writing to it,
- Ensure computer room equipment is not swapped around. That is, no changing of keyboards, mice or other equipment from one computer to another,
- Report all equipment faults to your teacher immediately, and
- Never trespass in another person’s computer folders.

Legal Implications
For legal purposes email has the same standing in court as paper documents. Users must be aware that the college can be involved in litigation. Records relating to use and activities involving email, internet and intranet can be requested by a court order or subpoena. These include matters affecting legal proceeding, affecting personal affairs of employees, parent, students, or third parties, as well as relating to research, or other communications even if communicated in confidence.

Email residing on or transmitted across the Glasshouse Country Christian College system is the property of the College. All electronic files are the property of the College, and users should act on the basis that they can be, and where necessary will be, held accountable for their messages and stored files.

While all transmissions remain the property of the College by law, all efforts to retain professional confidentiality will be made. Confidentiality is not guaranteed regarding private emails that are sent/received on the College system. All internet activity is recorded for individual users. Reports of this activity are continually being monitored. Over time, all employees and students could expect that the record of their internet activity will be viewed by senior staff of the College.

Employees: Should access to an individual’s files or internet logs be necessary for an alleged criminal offence or serious disciplinary matter the individual concerned will generally first be told the circumstances of the complaint and will be requested to be present when the files or logs are opened. The individual may be accompanied by their Union representative, or a colleague. Notwithstanding the above, the College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any College computer.

Students: Where there is an alleged criminal offence of serious disciplinary matter concerning a student, the individual concerned will generally first be told the circumstance of the grievance. Parents will be informed, and disciplinary actions taken. The College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any College computer.

**Acceptable Use Parameters**

Appropriate activities for acceptable use include:

- Correspondence with colleagues and contacts around the world via email
- Connecting to resources that provide a variety of academic and employment related information
- Exploring the internet looking for information and resources useful in carrying out academic and professional requirements
- Employees: Minimal amounts of personal correspondence with family or friends. This is a difficult area to determine acceptable quantities, but a rule of thumb would be that if an employee had to spend on average more than 10 minutes a day on non-employment related emails then this is an excessive amount.

**Unacceptable Use for College Employees and Students**

**Maintenance of Security**

- On no account should an employee or student pass on their login code or password to any other person, with the exception of IT employees or students to teacher.

**Damage**

- College employees and students must not damage computers, computer systems or computer networks; this includes removal and/or swapping of keyboards and/or other computer components.

**Defamation**

- College employees and students must not publish, post or include in an email any material which might be deemed to defame an individual, company or organisation.

**Improper Communications**
• Such as chain letters or other communications that are not in-keeping with the College ethos. Sending of improper communications may harm employees and students, and expose the College to risk of legal action or adverse publicity. Email must not be sent anonymously.

Commercial and other inappropriate use
• Use of the College computers/network/email for personal financial gain, unauthorised buying and selling of items, gambling purposes or other commercial purposes is prohibited.

Harassment
• College employees and students must not transmit, or cause to be transmitted, communications (whether in the form of text, picture or other data) that may be construed as harassment or disparagement of others based on the criteria of the anti-discrimination legislation and college policy.

Jokes
• Employees and students must not send emails which contain jokes and/or articles which are in poor taste; contain coarse language, racist or sexist comments.

Pornography
• Employees and students must not access, store or transmit pornographic material on College systems. When such material is inadvertently encountered, the employee or student must immediately exit from the site. In the case of the student their teacher must be notified. In the case of an employee their supervisor or Network Administrator must be notified. If this site has implications for searches, the Network Administrator must be advised of the unwanted site link.

Consequences of Unacceptable use:
Employees: Should access to an individual’s files or internet logs be necessary for an alleged criminal offence or serious disciplinary matter the individual concerned will generally first be told the circumstances of the complaint and will be requested to be present when the files or logs are opened. The individual may be accompanied by their Union representative, or a colleague. Notwithstanding the above, the College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any College computer.

Students: Where there is a serious disciplinary matter concerning a student, the individual concerned will generally first be told the circumstances of the grievance. Parents will be informed and disciplinary actions taken. The College reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any College computer.

Privacy Issues:
College employees and students must not include in documents or emails personal information about colleagues, students or parents without their written consent.
College employees and students should act within the GCCC Privacy Policy.

Forums/Listservs
Only employees of the College may subscribe to listservs, however they need to:
• Unsubscribe or suspend mail from listservs during holiday periods and periods of absence
• Be familiar with and follow the common rules of etiquette of that listserv
• Include a signature block in all postings
• Delete unwanted emails.

Copyright
Users must not:
• Download or authorise downloading of information or software from the internet or emails to provide to a third party
• Violate copyright, license agreements or contract of usage. This includes through the use of peer to peer file sharing sites.
• Undertake any action which might interfere with the integrity of data or a commercial software program e.g. introduce viruses

Respecting the systems’ limitations
College employees and students are requested to:
• Avoid sending large attachments, especially to the address, or other large distribution lists because of the impact on the network’s performance.
• Not send, forward and/or reply to large distribution lists concerning non-school business.
• Must consider the impact on the network when creating and using large distribution lists.
• Not forward lengthy or frequent emails to system groups, which may be time wasting or unwanted for many recipients.
• Avoid the use of decorative email screens. These can take up as much as 30 times the memory and disk space of an ordinary email.

Protection against viruses
College employees and students need to work in accordance with safe computing practices to minimise the risks associated with computer viruses.
Note:
• Be careful opening email attachments from unknown sources; if in doubt about a source, check with IT personnel.
• Never open .exe files.
• Should the virus protection software detect a virus from an incoming file, inform the person who introduced that file so they can ensure it does not happen again.
• If a computer is acting strangely, there may be an undetected virus. This does not happen often, but it is worth checking with the network team.

Conservation of electronic and print resources
Efforts must be made to conserve the finite resources of the College. This can be achieved through such behaviour as:
• Avoid using large amounts of the system resources such as disk space
• Avoid leaving programs open causing congestion of the network
• Always close down properly, avoiding system failures
• Avoid waste such as unnecessary broadcast messages or attaching large files to email messages
• Avoid printing straight from an internet site. Try to copy and paste the relevant section or use a database to keep track of your data.
• Endeavour to keep paper wastage to a minimum
• Before printing, proofread, spell check, and print preview your document, and only when completely satisfied with the document send it to the printer.
• Place unwanted printouts in recycling boxes.
• Email received on the College system is retained on the server until deleted by the recipient.
  To conserve disk space, maintain your mailbox by:
  o Keeping messages short
  o Checking email daily
  o Deleting unwanted messages immediately
  o Emptying your deleted messages wastebaskets frequently
  o Saving wanted messages to file rather than leaving them in the mail

Personal responsibility for security
System security is the individual and collective responsibility of all college users. All suspected security violations will be treated seriously as they may threaten the provision of the College service.
Any users who suspect a security problem on the College network including the internet must immediately notify the Principal and not demonstrate the problem to others. Any user who believes their
files have been tampered with must immediately change their password and contact the Principal with the specific details.
Acceptable Use of Technology Agreement

**Please sign and return this page only to your child’s pastoral care/form teacher.**

I/we have understood and agree to the abovementioned conditions set out in this document. I/we understand that my (my child’s) computer/iPad access at the College is not an automatic right and it can be withdrawn as a matter of course.

Student Name_________________________________________ Signed ___________ Date: ____________

Parent Name_________________________________________ Signed ___________ Date: ____________