Staff Internet and Email Usage Policy

March 2019

Date Approved	28 March 2019	**Number of pages**	8
Prepared by	Peter Fallon, Head of Senior School	**Date prepared**	March 2019
Approved by	K Newby-Acting Principal	**Monitored by**	Acting Principal
Reviewed by	Executive	**Date for next review**	March 2021

RATIONALE

These guidelines and requirements are in place to protect employees, students and the wider FCC community. Inappropriate use of the internet and email facilities exposes FCC to risks including virus attacks, compromise of network systems and services, neglect of duty of care and legal issues.

Internal network, Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, the wireless network and staff accounts are the property of FCC. These systems are to be used for educational and business purposes in serving the interests of the College.

Effective security is a team effort involving the participation and support of every FCC employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

SCOPE

This policy applies to employees, contractors, consultants, casual staff and visitors at Foundation Christian College, including all personnel affiliated with third parties.

POLICY

1. General Guidelines for Internet and Email usage

1.1 Introduction

The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the College's email facilities. You are encouraged to act with caution and take into account the underlying principles intended by this Policy. If you feel unsure of the appropriate action relating to use of email or the internet, you should contact your line manager or the Principal.

You should be aware that use of the College's computer network in a manner inconsistent with this policy or in any other inappropriate manner, will give rise to disciplinary action, including termination of an employee's employment or contractor's engagement.

1.2 College Property / Copyright

The College is the owner of copyright in all email messages created by its employees and contractors in performing their duties.

Copyright laws may also be infringed by employees who forward emails that contain material protected under copyright laws.

1.3 Monitoring

From time to time, the contents and usage of internet and email may be examined by the College or by a third party on the College's behalf. This will include electronic communications which are sent to you or by you, both internally and externally.

You should structure your email in recognition of the fact that the College may from time to time have the need to examine its contents.

The College's computer network is a business and educational tool to be used primarily for business or educational purposes. You therefore have a responsibility to use these resources in an appropriate, professional and lawful manner.

All messages on the College's system will be treated as education or business-related messages, which may be monitored. Accordingly, you should not expect that any information or document transmitted or stored on the College's computer network will be private.

You should also be aware that the College is able to monitor your use of the Internet accessed by College equipment at all times. This includes the sites and content that you visit and the length of time you spend using the Internet.

Emails will be archived by the College as it considers appropriate.

1.4 Defamation

Generally, defamation occurs when a person publishes a statement that harms or damages the reputation or standing of another person within the community. A statement is published once it is known by a third person. If an employee transmits an email to a third person and makes a statement about the other person’s reputation which is false, this publication may result in action against the employer for defamation. However, the employer may allege the defence of ‘innocent publication’ if they did not know that the email contained defamatory material.

1.5 Content / Sexual Harassment

The Sex Discrimination Act 1984 defines sexual conduct as, “conduct of a sexual nature includes making a statement of a sexual nature to a person, or in the presence of a person, whether the statement is made orally or in writing.” As a result, sexual harassment may also occur by the transmission of sexually explicit material or offensive jokes in emails or downloading pornography and sexually explicit material from the internet.

Email correspondence should be treated in the same way as any other correspondence, such as a letter or a fax. That is, as a permanent written record which may be read by persons other than the addressee and which could result in personal or the College's liability.

You and/or the College may be liable for what you say in an email message. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.

You should never use the internet or email for the following purposes:

- to abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other)
- to send or receive obscene or pornographic material
- to injure the reputation of the College or in a manner that may cause embarrassment to your employer
- to spam or mass mail or to send or receive chain mail
- to infringe the copyright or other intellectual property rights of another person
- to perform any other unlawful or inappropriate act

Email content that may seem harmless to you may in fact be highly offensive to someone else. You should be aware, therefore, that in determining whether an email falls within any of the categories listed above, or is generally inappropriate, the College will consider the response and sensitivities of the recipient of an email rather than the intention of the sender.

If you receive inappropriate material by email, you should delete it immediately and not forward it to anyone else. It would be appropriate for you to discourage the sender from sending further materials of that nature.

Comments that are not appropriate in the workplace or College environment will also be inappropriate when sent by email. Email messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

1.6 Privacy

In the course of carrying out your duties on behalf of the College, you may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email should not be used to disclose personal information of another except in accordance with the College's Privacy Policy or with proper authorisation.

The Privacy Act requires both you and the College to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. We stress therefore, that you take responsibility for the security of your personal computer and not allow it to be used by an unauthorised party, which specifically includes anyone who is not an employee of the College.

You will be assigned a log-in code and you will also select a password to use the College's electronic communications facilities. You should ensure that these details are not disclosed to anyone else. We suggest that you take steps to keep these details secure. For example, you should change your password regularly and ensure that your log-in code and password are not kept in writing close to your working area.

You are encouraged to either lock your screen or log-out when you leave your desk. This will avoid others gaining unauthorised access to your personal information, the personal information of others and confidential information within the College.

In order to comply with the College's obligations under the Privacy Act, you are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.

In addition to the above, you should familiarise yourself with the National Privacy Principles ('NPPs') and ensure that your use of email does not breach the Privacy Act or the NPPs.

1.7 Distribution and Copyright

When distributing information over the College's computer network or to third parties outside the College, you must ensure that you and the College have the right to do so, and that you are not violating the intellectual property rights of any third party.

In particular, copyright law may apply to the information you intend to distribute and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through email without specific authorisation to do so.

1.8 Encryption and Confidentiality

When email is sent from the College to the network server and then on to the Internet, the email message may become public information. Encryption will reduce the risk of third parties being able to read email and should be used in cases where you feel additional security is required.

As mentioned above, the Internet and email are insecure means of transmitting information. Therefore, items of a highly confidential or sensitive nature should not be sent via email. You should note that there is always a trail and a copy saved somewhere, not necessarily only on the College's network server.

This confidentiality requirement applies even when encryption is used.

Email sent over the Internet may be truncated, scrambled, or sent to the wrong address. There is a possibility that outgoing email sent over the Internet may arrive scrambled or truncated, may be delayed, may not arrive at all, or may be sent to the wrong address. Where outgoing email is important or urgent, you should verify that the recipient has received the email in its entirety.

1.9 Viruses

All external files and attachments must be virus checked using scanning software before they are accessed. The Internet is a potential host for computer viruses. The downloading of infected information from the Internet is potentially fatal to the College computer network.

A document attached to an incoming email may have an embedded virus.

Virus checking is done automatically through the virus protector software installed on the network server. If you are concerned about an email attachment, or believe that it has not been automatically scanned for viruses, you should contact your line manager.

1.10 Personal Use

You are permitted to use the internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with the performance of your work duties.

However, you should bear in mind that any use of the internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.

In the case of shared IT facilities, you are expected to respect the needs of your colleagues and use the Internet and email in a timely and efficient manner.

Excessive or inappropriate use of email or internet facilities for personal reasons during working hours may lead to disciplinary action.

2. Emails

2.1 General points

You must ensure that all emails that are sent from your email address contain the College's standard disclaimer message, which will read as follows:

“The contents of this email are confidential. Any unauthorised use of the contents is expressly prohibited. If you have received this email in error, please advise by telephone immediately and then delete/destroy the email and any printed copies.”

There is a risk of false attribution of email. Software is widely available by which email messages may be edited or 'doctored' to reflect an erroneous message or sender name. The recipient may therefore be unaware that he or she is communicating with an impostor. Accordingly, you should maintain a reasonable degree of caution regarding the identity of the sender of incoming email. You should verify the identity of the sender by other means if you have concerns.

Please delete old or unnecessary email messages and archive only those email messages you need to keep. Retention of messages fills up large amounts of storage space on the network server and can slow down performance. You should maintain as few messages as possible in your in-boxes and out-boxes. If there are items in your email which you require at a later date, please ensure that these are saved in your network directory so that appropriate backups are made College wide.

3. Internet Usage

3.1 General Use

While Foundation Christian College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of FCC. Because of the need to protect FCC's network, management cannot guarantee the confidentiality of information stored on any network device belonging to FCC. To that end, users must exercise discretion on information they store on FCC equipment.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

For security and network maintenance purposes, authorised individuals within FCC may monitor equipment, systems and network traffic at any time.

FCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security

Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed every six months, user level passwords should be changed quarterly.

3.3 Unacceptable Use

Under no circumstances is an employee of FCC authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Foundation Christian College-owned resources.

Unacceptable use includes but is not limited to:

- Games and game cheat sites, unless specifically for education purposes.
- Social Networking sites – using FCC resources for personal social networking that is not in the interests of the core business of the College.
- Sites that promote/enable inappropriate language or material that appears on your screen. If you are unsure about any images or sites – you should immediately advise the Principal and Head of School or Business Manager.
- Any sites as determined by the Executive of Foundation Christian College, through discussion and notification to not serve the interests of the College.

- Any website which is contrary to the Christian principles of the College i.e., that would expose FCC equipment, staff, students and community to risks including virus attacks, compromise of network systems and services, neglect of duty of care and legal issues.

4. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by FCC. This includes bit torrents or proxy bypasses for downloading pirated copies of digital media
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which FCC or the end user does not have an active license
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, malware etc.)
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home
- Using FCC equipment and/or network to actively engage in procuring or transmitting material that is in violation of sexual harassment laws, or hostile workplace laws in the user's local jurisdiction
- Making fraudulent offers of products, items, or services originating from any FCC account
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- Port scanning or security scanning is expressly prohibited
- Executing any form of network monitoring which will intercept data not intended for the employee's host
- Circumventing user authentication or security of any host, network or account
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet
- Providing information about, or lists of, FCC employees to parties outside FCC that could be used for activities other than interests of the College or the individuals

5. Terms and Definitions

Some of the terms used throughout the policy are explained below:

Bit torrents - A protocol for the practice of peer-to-peer file sharing that is used to distribute large amounts of data over the Internet.

Proxy Bypass - The act of sending traffic through another provider to obtain internet data. Usually used to avoid firewall or content filtering restrictions

Worms - A standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.

Trojan horse - A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage.

Email Bombs - A form of internet abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Malware - Short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software

Network sniffing - A computer tool that captures data sent across a local network.

Pinged Floods - A denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets.

Packet Spoofing - The creation of Internet Protocol (IP) packets with a source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.

Denial of Service - An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.

Forged Routing - The act of broadcasting false routing information

Port Scanning - A software application designed to probe a server or hosts for open ports

Chain letters - One of a sequence of letters, each recipient in the sequence being requested to send copies to a specific number of other people.

Agreement to abide by the Staff Internet and Email Usage Policy

I have read, understood and agree to comply with the Staff Internet and Email Usage Policy, as laid out in this document.

I understand and agree that the school has the right to and may monitor staff use of the internet, email and social media at any time.

Staff Name: ______________________________

Staff Signature: ______________________________ Date: ______________

Please provide this signed page to the Principal or Business Manager.

To be placed in staff personnel file