uniting church
in Australia,
Synod of NSW & ACT

Internet & Email Policy

Title: Internet and Email Policy
Creation Date: August 2021
Version: 0.1
Last Revised: March 2022
Approved by: Synod Office SLT

Table of Contents

1. Overview/Background

Email and internet are wonderful tools of trade with the power to either support our communications, information sharing and productivity or to cause harm.

There are many laws which touch email and internet usage and, through the development of this policy, we have endeavoured to provide some easy-to-follow rules, most of which are common sense. Notwithstanding that, there are some traps which can be easy to fall into (e.g. copyright breaches) without a raised awareness. We hope this policy supports you in correctly managing email and internet usage.

2. Purpose of Policy

This policy outlines the Synod's requirements in relation to individuals' use of the Synod's email and internet services. The policy is part of a suite of policies which govern technology, privacy, surveillance, social media and appropriate workplace behaviour and therefore should be read in conjunction with those policies.

3. Applicability (scope)

This policy applies to:

- All employees, Ministers, volunteers and independent contractors ('**individuals**') of the Synod of NSW and ACT ('**Synod**')
- All use of Internet and email services where that use is undertaken through the Synod's information technology environment, network, systems, services and devices, regardless of the location from which it is accessed. As a result, this policy applies equally when working in the office, at home or other remote location.

4. Responsibilities

4.1 Policy Owner and Sponsor

Information Technology ('**IT**') own this policy and are responsible for:

- Implementing and overseeing the policy;
- Educating individuals as necessary and ensuring they are aware of their obligations under this policy;
- Running regular checks and monitoring and keeping IT devices, systems and services up-to-date;
- Consulting with People and Culture in relation to any policy breaches.

4.2 Individuals

Individuals are responsible for understanding and complying with this policy and remaining vigilant to the matters contained herein.

5. Principles

5.1 Use of the Synod's network services, systems and devices

Internet and email services, systems and devices are provided by the Synod for business use however the Synod understands that, from time to time, particularly as we work more flexibly,

individuals may use Synod networks in the course of attending to personal obligations or needs.

There is a reasonable limit to which the Synod's internet and email services, systems and devices may be used for personal purposes and individuals are expected to exercise good judgement both in terms of time spent on personal use and in the nature of that use.

Regardless of the reason for use, all individuals have a responsibility to act ethically, legally and responsibly at all times in their use of the Synod's IT systems, services and devices.

Failure to comply with this policy could lead to disciplinary action up to and including termination of employment and, in some circumstances, legal action.

5.2 Surveillance, monitoring and tracking

All files contained on the Synod's IT services, systems and devices are the property of the Synod. As such, the Synod has the right to access and audit emails and files on its systems, services and devices for compliance with relevant legislation and policies.

Further information can be found in our Workplace Surveillance Policy.

6. Responsible Use of Internet and Email

At any time when using Synod IT services, systems and devices, an individual is representing the Synod and, as such, has the ability to enhance or damage the Synod's reputation.

It is each individual's responsibility to ensure that the content of any e-mail written by them complies with current legislative requirements and:

- cannot be construed as being discriminatory, defamatory, harassing or vilifying; and
- doesn't infringe on copyright or amount to plagiarism.

As it is possible to form a legally binding contract by e-mail, it is each individual's responsibility to exercise caution when corresponding via e-mail with parties regarding Synod matters, suppliers and vendors.

Further, as every site and application we visit leaves traces of us, whether we have interacted or not, individuals need to exercise good judgement when using the internet.

6.1 Unsolicited and suspicious emails

Beware of unsolicited emails which can contain viruses or trojan horses or which are phishing (or similar) attempts. If you receive an email from an unknown sender or an unexpected email from a known sender and it looks suspicious, don't open the email, reply or click on any links or attachments within it. Email scams have become increasingly sophisticated often mimicking someone we know. Always take a close look at the sender's email address (not just email alias) before actioning any email.

6.2 Free web-based email accounts and file sharing software

Free web-based accounts and file sharing software may be owned by international companies in foreign jurisdictions with differing legislation applied to the information. Examples of free web-based email accounts include, but are not limited to:

- Gmail;
- Hotmail;
- Yahoo!

Once information has been sent to web-based email accounts or uploaded onto file sharing programs, it can often no longer be controlled.

Under no circumstances should Synod (or associated entities of the Synod) information be sent by individuals except from authorized Synod devices, systems and software.

7. Inappropriate and Unlawful Use of Internet and Email

The use of the Internet or email to make or send fraudulent, unlawful, offensive or abusive information or messages is prohibited. Individuals are to report receipt of any such messages to their People Manager or Director. Any individual who initiates or shares such information or messages is subject to disciplinary action up to and including termination of employment. Depending on the circumstances, referral to the relevant law enforcement or government agency could also occur.

Unlawful and inappropriate use of the Internet and email includes, but is not limited to, creating, sending, communicating, sharing, storing or accessing information that:

- Could damage the reputation of the Synod;
- Could be misleading or deceptive;
- Could lead to criminal penalty or expose the Synod to civil liability;
- Facilitates unauthorised access, modification or impairment of data on a computer;
- Could be reasonably found to be offensive, obscene, threatening, abusive or defamatory;
- Is pornographic or sexually explicit including images, text or other offensive material;
- May discriminate against, harass or vilify individuals or any member of the public.

In addition to the above, the following activities are also prohibited:

- Individuals representing themselves anonymously or as someone else (whether real or fictional) when sending emails or posting information to the internet or social media sites;
- Using another individual's email account to send emails (unless given explicit information to do through the use of Outlook permissions);
- Using another individual's account to access the internet, this includes sharing any credentials allocated to you by the Synod;
- Undertaking any form of computer hacking;
- Sending or forwarding chain mail;
- Using their Synod email address to subscribe to non-work-related sites or events;
- Using the internet or email activities for sites such as gambling, gaming, TikTok, accessing chat lines;
- Using Synod email address or logo to create the impression that a personal viewpoint is that of the Synod;
- Downloading or streaming movies, music or news services, however we do not place restrictions on individuals reading news from appropriate news sites;
- Transmitting any Synod information to media organisations or to the general public unless expressly authorized to do so as part of their role and responsibilities.

8. Streaming, Downloading and Uploading

As well as the potential to clog and slow down our internet and email services, streaming, downloading and uploading could result in copyright infringements. To avoid falling foul of the law, the Synod applies the following rules:

- The streaming of, downloading from and uploading to the internet of video and music files is prohibited unless it is work-related and has been approved by an individual's People Manager.
- Certain file types may be automatically blocked. Where an individual has need of a blocked file for the purposes of their work, they are asked to contact IT, outlining the need for the file in order to have it released.
- As software has the potential to bring in viruses, unauthorised software is not to be downloaded under any circumstances. Individuals requiring access to additional software are asked to obtain the approval of their People Manager, outlining their need for the software, and then liaise with IT once granted. This process must be followed regardless of the licence type, including free trials.

9. Security and Privacy

9.1 Monitoring and Privacy

The use of Synod systems and devices (including but not limited to computers, tablets and phones) is monitored through a user ID and password.

Individuals are responsible for all Internet activity and email use logged against their user ID. To prevent unauthorised use of their user ID and to protect their privacy, individuals are asked to:

- Lock their computer when they're away from it. This is important at all times but particularly so when working from home or other remote location;
- Not to disclose their user credentials to anyone else;
- To ensure that any individuals who've been granted permission to send email or meeting invitations on their behalf are aware of the limitations and responsibilities associated with that use.

Email is not a confidential means of communication. While we recognise and respect privacy of email communications, messages conveyed by email and through the Internet are capable of being intercepted, traced or recorded by others. Although such practices may be illegal, individuals can't expect the privacy of communications to be respected and must take care with confidential documents. Further, in the event of any legal or other actions, emails are discoverable and even deleted emails can be recovered.

9.2 Information Security

In the course of our work, we are sometimes in possession of confidential or sensitive information and care must be taken when receiving or transmitting information to others. Release of private or sensitive information, whether accidental or intentional, is a potential breach of the Privacy Act (1988) Cth and could carry serious consequences.

Please see our Privacy Policy for further information.

10. Legislation and Policies

Legislation

The Privacy Act (1988) Cth
Workplace Surveillance Act (2005) NSW
Discrimination, Harassment and WHS laws
Copyright Act (1968) Cth

Policies

Code of Conduct and Ethics
Bullying, Harassment and Discrimination policy
Social Media policy
Privacy policy
Workplace Surveillance policy

11. Terms and Conditions

This Policy does not form part of any contract of employment or contract of engagement and may be amended, replaced or revoked at any time by the Synod at its discretion.