

Parish Electronic Communications Policy

Objective/Intent

This policy is designed to ensure the prudent use of electronic communications including internet and email, so that all employees and volunteers are provided with a safe working environment and the Parish is protected from commercial harm.

Background

Electronic communications utilising emerging technologies opens up vast opportunities for sharing information and conducting parish business. However this also brings with it an obligation to manage the risks associated with the use of these technologies in a coordinated way so as to minimise the risks.

Employees and volunteers should be aware that although there are access passwords and the like there is general “insecurity” for communications via the Internet and email.

Electronic Communication includes but is not limited to:

- World Wide Web pages
- Electronic journals and texts
- Library catalogues
- Email
- Discussion lists
- Internet relay chat
- Data of all kinds

Policy

Personal Use

All use, personal and business, must be appropriate and lawful. Personal use that is excessive and affects the employee’s performance is considered inappropriate.

This technology is primarily for parish related use and be used in accordance with the guidelines set out in this policy. The Parish recognises that a restricted and discreet use of electronic services may occur, as with telephone calls, for private purposes.

Personal use of these facilities must be lawful, must not interfere with your ability to perform your contract of employment or to otherwise fulfil your obligations to the Parish and must not interfere with or adversely impact on the reputation of the Parish or others in the workplace.

Personal use of these facilities for operating or promoting a personal business venture or other business venture is prohibited.

Passwords and Password Confidentiality

Do not interfere with any password.

It is prohibited for any employee to:

- share their password/s with others
- hack into other systems
- read or attempt to determine other people's passwords
- breach computer or network security measures
- monitor electronic files or communications of others unless authorised to do so, or
- write their password down.

You may upon request be expected to disclose your password/s to an authorised IT person for system maintenance and security.

Identity

No email or other electronic communication may be sent which conceals or attempts to conceal the identity of the sender.

The only exception is where part of a systems functionality is intended to keep the identity of the sender anonymous, such as feedback forums or electronic surveys that may be conducted by from time to time.

Confidential Messages

Do not send highly confidential messages via the Internet or email.

Always exercise care and discretion with electronic communications.

Email messages are perceived to be instant in nature and instantly disposed of. In reality they are retained by both the recipient and the sender until specifically disposed of and then only usually into what is called a trash file. There may also be an additional backup facility that retains the message for a period of time. It is often stored onto a backup tape as routine data protection. This backup tape is a copy of the file even if it is eliminated from the sender's and recipient's computers.

Improper statements can give rise to liability — personally and for the Parish.

Employees should work on the assumption that messages may be sent, forwarded, or transmitted to someone other than who you intend to receive or read your message. Controlled or limited distribution of your messages cannot be guaranteed.

Employees should be very cautious about committing totally private, sensitive or confidential messages to electronic communication.

Users should also be aware that email messages, even if expressed to be confidential, may have to be disclosed in Court proceedings, Freedom of Information requests, or in investigations by competition authorities and regulatory bodies.

Court requirements for discovery of documents are not overcome by the fact that an email is stored in electronic form. It may be necessary for parish employees or third parties (under Court or regulatory body appointments) to retrieve and/or disclose such documents.

Virus Protection

Do not import non-text files or unknown messages into your system without having them scanned for viruses.

Email attachments are common. Virus infection is most prevalent in non-work related emails.

Clearance should be sought for any doubtful attachments.

Under no circumstances should employees open a .zip or .exe file without first referring it for clearance.

Do not act on any emails no matter how official they look unless you are sure the email is legitimate. If unsure please ask.

Some questions to ask yourself to help identify unsolicited or junk emails which may contain a virus are;

1. Who is the email from?
2. Do I recognise the sender and their email address?
3. Does the subject make sense?
4. Am I expecting an email from this person or on this subject?
5. Are there any spelling, grammatical or typographical errors-this usually suggests the email is not official or from a foreign country where the author does not have a good grasp of English.
6. Are there attachments to the document with .zip, .exe or double file extensions such as .doc.exe - these attachments should be considered suspicious.

Finally be sure to delete the email permanently from you deleted items folder.

Confidentiality Clause

All documents must contain the standard parish confidentiality clause.

The purpose of a confidentiality clause is to impress on any unintended recipients notice of the confidential nature of the document. Employees should ensure their standard email template contains the parish confidentiality clause.

Unlawful Activities

Do not access or send material that is prohibited or potentially prohibited, provocative, pornographic, offensive, abusive, sexist or racist. Likewise, do not forward to others any that you receive.

Unlawful activities are absolutely prohibited. They include:

- gaining access to any material which is prohibited or potentially prohibited, pornographic, offensive or objectionable;
- engaging in any conduct which offends Federal or State laws and regulations; embarrassing, bullying or harassing (sexually or otherwise) another person;
- engaging in any defamatory message - including reading and then forwarding a message of which you are not the author;
- sending or forwarding any material which is defamatory, abusive, sexist, racist or otherwise illegal;

- circumventing any filtering or other content access device or software;
- interfering with electronic rights management information.

This includes the transmission of jokes, anecdotes, song lyrics or animated and graphic images. There are serious repercussions arising from such transmission including offences under the *Broadcasting Services Amendment (Online Services) Act 1999* and the *Spam Act 2003*. Employees should note that these activities may also involve a breach of their obligations pursuant to their employment contract and Conditions of Employment.

Defamation

Do not be a party to or participate in the trafficking of any defamatory message.

To defame someone, you must publish a statement that is or is likely to cause the ordinary, reasonable member of the community to think less of the defamed person or to injure that person in his or her trade, credit or reputation.

For the purpose of defamation law “publication” is very broad and includes any means whatsoever that we use to communicate with each other — including Internet and email. A statement made electronically is, by its every distribution, published. A statement is also published if it is simply received electronically and forwarded on electronically. The Parish may be at risk of being sued for any defamatory material stored, reproduced or transmitted via any of its facilities. Likewise, an individual may also be sued.

Copyright

Beware of copyright requirements.

Intellectual property rights apply to most material on the internet, including text, graphics, clip art and sound. Employees must respect these rights.

Employees should not assume that they can reproduce, print, transmit or download all material to which they have access. Employees have rights to use material consistently with the technology or the rights of the owner of the material.

Material reproduced outside permitted uses or without the permission of the owner may be unlawful and may result in legal action against the employee and Parish.

Privacy Act

Beware of privacy requirements.

Information of a personal or sensitive nature can only be used for the purpose in which it is given. Employees must respect these privacy principles.

Employees should not assume that they can reproduce, print, transmit or download private information to which they have access.

Private information reproduced outside permitted uses or without the permission of the individual may be unlawful and may result in legal action against the employee and Parish.

Hard Copies

Emails are parish correspondence and the standards and record management practices, procedures and protocols applying to letters apply equally to emails and any attachments. Employees are encouraged to obtain confirmation of receipt of important messages.

Employees should make hard copies of emails that need to be retained for record keeping purposes. This is simply a matter of good practice and common sense. People often fail to make hard copies of messages they send or receive which may later require retrieval. A reply email for important communication is recommended.

Breach of Policy

The conditions of this policy must be strictly adhered to. If an employee breaches any conditions of this policy the Parish reserves the right to terminate the employees' use of the technology, equipment or services and to maintain that restriction in its absolute discretion.

Serious, wilful or neglectful abuse or misuse of the technology or equipment by employees may result in warnings or disciplinary proceedings.

Any material sent, received, forwarded or transmitted may from time to time be subject to retrieval by the Parish if it believes any use of electronic communication by the employee;

1. Is illegal;
2. Is affecting the performance of the employee or;
3. Is not in the best interest of the Parish.

Indemnity for Non-Employees

The Parish bears no responsibility whatsoever for any legal action threatened or commenced due to conduct and activities of non-employees (including family members) in accessing or using these resources or facilities. All employees indemnify the Parish against any and all damages, costs and expenses suffered by the Parish arising out of any unlawful or improper conduct and activity by their family members, and in respect of any action, settlement or compromise, or any statutory infringement caused by their family members.