Electronic Communication

Policy Statement:
The purpose of this policy is to provide Echuca Regional Health (ERH) staff with information and acceptable use guidelines to allow equitable, effective, ethical, safe and efficient use of ERH email systems and other Internet based services.

ERH supports and encourages the responsible use of email as an effective business communications tool. Internet services provided at ERH are made available to afford staff greater access to information resources, online tools, forums or services and its use for productive business purposes is encouraged. While reasonable personal use of these services is permitted, these services have not been provisioned for the promotion of personal business or private enterprise and must not be used in breach of state, federal or copyright laws.

This policy applies regardless of what device (computer, laptop, tablet, smartphone, PDA, Android box, micro-computer, thin client etc.) is used to access online services and regardless of the means of connection to the ERH computer and data network infrastructure.

Definitions:

Email: A message comprised of text, images diagrams, or other informational content, created, sent, forwarded, replied to, or transmitted via the Internet.

ERH email address: An ERH email address contains @erh.org.au at the end of the email address.

ERH email system: Server hardware, data storage and software required to provision email services.

ERH Network Infrastructure: Any copper or fibre network cables, ADSL, GWIP or fibre based Internet connections, network switches, firewalls, routers or wireless equipment owned and operated by ERH ICT and usable to connect a computer to the Internet and any other computers or computer & data systems.

External Recipient: someone who receives an email, but works for a different organisation than the sender. The sender and receiver have email addresses where the text after the '@' symbol is different.

Liquidfiles: is an add-on to Microsoft Outlook that allows large and confidential files to be sent to external recipients securely to avoid breaching privacy and confidentiality responsibilities.

Online Services: Internet based information systems and services accessible via a web browser, cloud storage, Usenet, wiki's, social media and multi-media/entertainment platforms.

P2P: Peer-to-peer. A class of software which facilitates the exchange of files directly between computers connected to the Internet.

Phishing email: a method of stealing confidential information by sending fraudulent messages to a victim. The messages often contain a link to a bogus website where victims are coaxed to enter personal details such as logon information. Phishing emails appear to be from a known and trusted source, but the links and attached files are designed to bypass security measures.

SOE: Standard Operating Environment – a collection of software applications pre-installed or approved for installation on ERH desktop, laptop or mobile computers

Staff: ERH employees

Users: Persons using ERH Network Infrastructure to connect to or access online services.

Personnel to which this policy applies:
This policy applies to all ERH employees with an ERH email address and all consultants, contractors, students or volunteers who may require access to online services of any nature via any part of the ERH network infrastructure. This also applies to Users staying in the accommodation residence, which may be using their own personal computers to access the Internet using ERH Network Infrastructure.

Procedure:
Email Service
Principles of General Use
All Users of the ERH email system are responsible for ensuring that they use email in an ethical and considerate manner which does not compromise ERH's reputation or the security and integrity of ERH's data and information systems. The following points identify the principles of general use:

- The ERH email system is shared by over 1000 people. Limits are applied to user's mailboxes to ensure that system capacities are not exceeded or systems performance adversely impacted. Users should attempt to maintain their email in a manner that allows these limits to be sustained. The ERH email system will automatically generate warning notifications to users who breach any of the three email storage threshold limits. Failure to address storage notification messages will result in the ability to either receive or send emails being disabled by the system.
- Emails can be stored in archive files to avoid destroying corporate email documents. Arrangements can be made to have one or more archive folders created via the ICT (Information Communication & Technology) helpdesk.
- There is a limit to the total size of attachments that can be sent via email. An email cannot be sent via the ERH email system if all the attachments have a combined size greater than 35MB (Megabytes). If emails with attachments greater than this need to be sent, alternative options such as Liquidfiles should be discussed with ICT staff.
- Staff are prohibited from sending chain letters/messages or from sending or forwarding unsolicited bulk emails (including attachments) otherwise known as spam.

- Users should be vigilant for phishing and malicious emails. The majority of cyber-attacks originate from emails containing links or attachments capable of installing dangerous software or stealing a user's logon details. Refer to the Cybersecurity eLearning training module for more information regarding phishing and malicious emails.
- If you are suspicious of an email, please contact ICT for assistance in verifying the safety of the email
- Usernames and passwords must not be sent via email due to the risk of the details being stolen during transmission and potentially used to gain unlawful access to ERH computer systems.
- The ability to access email from a web browser operating on any computer (Outlook Web Access - OWA) represents a responsibility for Users to:
  - Ensure they use the log off button in the webmail session immediately following use – not just closing the web browser
  - Change email password regularly in accordance to ERH password policies and procedures
- The ERH email system is not to be used for unlawful activities or activities in contradiction to the ERH Code of Conduct Policy & Procedure including:
  - Sending or forwarding emails that contain but not limited to defamatory, offensive, racist, sexist, harassing, bullying or obscene statements, jokes or images
  - Forging or attempting to forge or disguise your email identity
  - Send an email using another person's account without the appropriate authorization
- Users are advised to notify the ERH ICT department if they receive an email that contravenes this policy.

Privacy & Confidentiality

All ERH staff need to be aware that email on its own, is not a secure method of communication. Emails can be intercepted between the sender and the receiver when the receiver is not in the same organization, and modified, copied or forwarded to others. For this reason, patient, financial or other private and confidential information which is covered by the ERH Privacy Policy & Procedure should not be sent using email.

Liquidfiles can be used to securely transmit private and confidential information to external recipients using email. Information on Liquidfiles use is available on the Intranet.

Personal Use

Emails and any attachments sent or received by the ERH email system are electronic documents which are corporate records and the property of ERH.

ERH acknowledges that staff may wish to use the ERH email system for occasional personal emails. This use is acceptable providing that:

- It is not for the promotion of personal business or private enterprise
- Does not breach state, federal or copyright laws
- Personal views are clearly identified as such
- It does not impact in any way on the Users ability to perform their required duties or waste time

Email Signature
Users sending emails from the ERH email system are perceived as reflecting the character and professionalism of ERH. As such, all users are required to use an ERH standard email signature, as prescribed by the ERH Document Style Guide (located on the Intranet at http://intranet/Resources/Documents/ERH%20Style%20Guide%20-%202015.pdf).

The email signature format is as follows:

<First Name Last Name >
<Job title/description>
Echuca Regional Health
226 Service Street, Echuca, Victoria 3564
<Days Working>
P 03 5485 5xxx
F 03 548x xxxx

Echuca Regional Health

Supporting Everyone to Be Healthy and Live Well

DISCLAIMER: This e-mail and any attachments may be confidential. You must not disclose or use the information in this e-mail if you are not the intended recipient. If you have received this e-mail in error, please notify us immediately and delete the e-mail and all copies.
Echuca Regional Health does not guarantee that this e-mail is virus or error free. The attached files are provided and may only be used on the basis that the user assumes all responsibility for any loss, damage or consequence resulting directly or indirectly from the use of the attached files, whether caused by the negligence of the sender or not. The content and opinions in this e-mail are not necessarily those of Echuca Regional Health.

The email signature needs to be applied to all emails.

Consent
As part of the employment process, ERH employees are required to sign a 'Code of Conduct'. Additionally, every time a person logs onto an ERH computer, the below notice appears with an 'OK' button at the bottom which users must click to acknowledge that they have read, understood and will abide by this and other ERH policies that are relevant to the use of ERH data and information systems.

I agree that I will use this computer for work-related purposes only. I have read, understood, and will abide by the ERH Electronic Communication Policy and the Computer Access Policy. Under these policies the accessing of offensive, discriminatory or sexually explicit material together with streaming media, social networking, gambling and file sharing services is strictly prohibited. I understand that failure to comply with these policies may result in disciplinary action up to and including termination.

Email Monitoring
ERH respects the privacy of its staff and does not, nor is obliged to, routinely inspect, retrieve, disclose or monitor the contents of emails. ERH reserves the right to do so under the prescribed conditions as follows:

- There is reason to believe that ERH policies may have been breached
- Compelling circumstances
- System recovery or backup restore
- As requested by law enforcement officials in consideration of the Privacy Act

In instances where the contents of a User's email needs to be examined for any of the above reasons, or access given to another in the absence of that Users consent, written consent will be required from the Human Resource Manager or a member of the Executive.

ERH ICT staff monitors the ERH email systems for the purpose of systems management, problem resolution, maintenance and capacity & performance planning.

Internet Service
Principles of General Use

Internet access is provided via ERH Network Infrastructure as a valuable tool to assist staff in work processes and as an information asset. The principles of general use are:

- Users are responsible for ensuring that they use the Internet in an ethical and considerate manner which does not compromise ERH's reputation or the security and integrity of ERH's data and information systems.
- Internet access is provided as a tool in support of business functions and not for the promotion of personal business or private enterprise.
- The Internet is not to be used to breach state, federal or copyright laws. It is reasonable to expect that materials found on the Internet are copyright and as such should be referenced if used.
- It cannot be assumed that all information on the Internet is correct. Users are responsible for conduction research thoroughly and validating Internet based sources of information.
- Downloading and installing software from the Internet without the express approval of ERH ICT is prohibited due to the potential of the software to:
  - conflict with applications forming part of the ERH Standard Operating Environment (SOE);
  - introduce system instabilities or;
  - compromise the security of ERH data and information systems.
- Using the ERH Network Infrastructure to access, download, stream or upload materials protected by copyright laws is prohibited.
- The use of all forms of peer-to-peer (P2P), BitTorrent or software download managers such as 'couchpotato' or 'sickbeard' to access and download copyright protected materials via the ERH Network Infrastructure is prohibited regardless of whether ERH computers are used or not.
- The use of ERH Internet services to access or transmit information or images that is obscene, threatening, offensive, pornographic, harassing, racist, discriminatory or contradictory to the ERH Code of Conduct Policy and Procedure is prohibited.
- The ERH Internet service can be used by staff for incidental personal purposes provided that it does not:
  - Interfere directly or indirectly with the operation or security of ERH data and information systems
  - Contravene stat, federal or copyright laws
  - Contravene the ERH Code of Conduct Policy and Procedure
  - Interfere with normal work responsibilities or waste time
- Use of ERH Internet facilities to engage in activities that could result in unauthorized access to another individual or organisations computer or information systems, otherwise known as hacking, is strictly prohibited.

Internet Monitoring
Internet usage including websites accessed and time spent at those sites is logged for all ERH Internet users. Monitoring and review of these logs may occur without prior notice to users in the interests of:

- Determining and maintaining operational efficiency and reliability.
- There is reason to believe that ERH policies may have been breached
- Compelling circumstances
- As requested by law enforcement officials.

Online Cloud Storage
A range of online or cloud-based storage options are available for people to store, transmit and share information with others. Popular examples include Dropbox, One Drive, iCloud and Google Drive. While these services can be useful, it is not permitted to use these online storage services for unencrypted ERH patient information or other information that is protected by the ERH Privacy Policy & Procedure. Data stored on many of the popular cloud storage solutions can be encrypted, making the storage of information secure. ERH recommends that if cloud storage is required to collaborate or share private and confidential information with others then the information must be encrypted. Please see ICT for further information.

Policy Violation
Users who contravene this policy will be subject to disciplinary action according to the ERH Disciplinary Policy. Additional consequences may include:

- Suspension of ERH computer access
- Initiation of legal proceedings.

References
Information Privacy Act (2000)
Copyright Act 1968
Cybercrime Act 2001
Crimes (property damage and computer offenses) Act 2003
Telecommunications Act 1997
Equal Opportunity Act 1995
Sex Discrimination Act, 1984
Racial Discrimination Act 1975
Disability Discrimination Act 1992
Human Rights and Equal Opportunity Commission Act 1986

Linked documents
Disciplinary Policy
Code of Conduct Policy & Procedure
Privacy Policy & Procedure
Computer Access Policy
Mobile Device Policy
ICT End-user Device SOE Policy

Accreditation Framework and relevant section
National Safety and Quality Health Service Standards 1

Revision History:

Date Issued:	19/12/2013
Date of Last Review:	September 2021
Original author:	ICT Manager
Stakeholders:	Mitch Parsons, Nick Pell, Adam Jerkin
Date of Next Review:	September 2025
Approved By:	Corporate Policy and Procedure Committee