Email Acceptable Use Policy

Policy Statement:

Echuca Regional Health (ERH) supports and encourages the responsible use of email as an effective business communications tool. The purpose of this policy is to provide users of the ERH email systems with information and acceptable use guidelines that protect the confidentiality of our patients, the reputation of ERH and its employees and the health service from security breaches or legal liability arising from breaches of other state or federal laws.

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.

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.

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.

Spam: also referred to as junk email, spam mail, or simply spam, is unsolicited messages sent in bulk by email (spamming)

Web mail: an ERH user can access their ERH email from anywhere using a web browser.

Users: includes all full time, part time and casual employees, including consultants, contractors, students, volunteers and Board Members.

Personnel to whom this policy applies:
This policy applies to all ERH employees and Users of the ERH email system.

This policy applies regardless of what device (personal or ERH provided computer, tablet or smartphone) is used to access and use the ERH email services.

Policy Acceptance

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 Email 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 and may result in disciplinary action up to and including termination.

Principles of General Use

All Users of the ERH email system are responsible for ensuring that they use email in a professional, lawful, effective and considerate manner which does not compromise ERH's reputation or the security and integrity of ERH's information systems.

The principles of general use are:

- The ERH email system and all messages sent, received and stored in it including personal email messages are the property of ERH.
- Each staff member is responsible for their email account including the safeguarding of access to the account.
- Each staff member is responsible for managing their mailbox, ensuring that emails are read, deleted and stored in a manner consistent with the mailbox limits.
- 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. Automatic system generated alerts will be sent to a User if their mailbox capacity is nearing full. Users are to take appropriate action if they receive one of these alerts.
- Staff are prohibited 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 malicious links or attachments capable of installing dangerous software or stealing a user's logon details. Refer to the

Cybersecurity eLearning training modules for more information regarding phishing and malicious emails.

- If you are suspicious of an email's origins or its content, please use the "Report Phish" button in Outlook to report the email. Alternatively, contact ICT for assistance in verifying the legitimacy or safety of the email or its attachments.
- 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). Liquidfiles is available to use if emails with attachments greater than this need to be sent. Please check the Intranet for information on how to use Liquidfiles to send large attachments.
- 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 any web browser on any computer 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/computer passwords 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, the Code of Conduct for the Victorian Public Sector, or applicable state or federal laws 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 (delegated 'Send on Behalf of' feature)
- Users are advised to notify the ERH ICT department if they receive an email that contravenes this policy.
- Email accounts are deleted when a staff members employment at ERH ceases.

Privacy & Confidentiality

All ERH staff need to be aware that email on its own, is not a secure method of communication and should not assume that the emails they send are private and confidential. Emails can be intercepted between the sender and the receiver and modified, copied or forwarded to others. For this reason, patient identifying information including images, financial or other sensitive information which is covered by the ERH Privacy Policy & Procedure should not be sent to external recipients using either the ERH email system or any other personal email service.

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 user's 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

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 retrieve email content for specific legitimate reasons such as recovery of lost messages or from system failure, compliance with investigations of wrongful acts or to meet statutory requirements. Email content retrieved under such circumstances will be at the direction of a member of the ERH Executive.

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

Policy Violation

Misuse of the ERH email service and breach of this policy or applicable laws will be treated as misconduct and 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
Password Authentication Policy
Mobile Phones 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:	February 2024
Original author:	Brent Colbert
Stakeholders:	ICT, Executive Director Finance & Corporate Services
Date of Next Review:	February 2027
Approved By:	Corporate Policy and Procedure Committee