Please note: This Procedure is currently under review by ISG as part of a Transalpine approach to policy alignment with the CDHB. If you have any questions regarding this document please contact the Chief Information Officer in the first instance.

1. Purpose

This Procedure outlines the process for the use of Email services throughout West Coast District Health Board (WCDHB) Facilities.

2. Application

This Procedure is to be followed by all staff members of the WCDHB.

3. Definitions

For the purposes of this Procedure:

User is taken to mean any individual having authorised access to WCDHB network or computer systems, whether internally or externally.

Download is taken to mean the process to save a file from an external source on to WCDHB information and computer systems.

Spam (noun) is taken to mean unwanted e-mail of a non-work related nature.

Spam (verb) is taken to mean the sending of an unwanted e-mail of a non-work related nature.

4. Responsibilities

For the purposes of this Procedure:

All *Email Users* are required to:
- ensure they abide by the requirements of this Procedure.

5. Resources Required

This Procedure requires:

i) WCDHB communications facilities

6. Process

1.00 The Email is an important part of the WCDHB operational activity. It provides communication channels, sources of information, and opportunities for interaction between WCDHB, other health service providers, consumers, and business partners. The WCDHB recognises the importance of providing secure and efficient Email capability to its staff members for their use in meeting business goals.

1.01 Like a letter or memo, an email message can be treated as a legal document and may be produced as evidence during legal proceedings.

1.02 Where technically possible, access to email by WCDHB staff members will be on the basis of identification and authentication of authorised users.

1.03 All WCDHB staff members shall:
   i) primarily use email for official WCDHB business;
   ii) be permitted occasional use other than for business purposes provided it:
      a) uses only a trivial amount of resources;
      b) doesn't interfere with staff productivity;
      c) doesn't pre-empt any business activity;
      d) does not embarrass or disadvantage WCDHB in any way;
      e) is not used for any other business or charitable endeavour.
      f) take care to ensure that they do not Spam, or send Spam, to other WCDHB users.

   iii) include a disclaimer on material or content published which identifies WCDHB in any way as the originating point of the material, saying that it is not necessarily a statement or opinion of WCDHB's, unless the author has obtained approval from the Chief Executive Officer for such publication;
   iv) treat email messages sent from any WCDHB email service as property of the WCDHB;
   v) treat email messages as business records. Retention, archiving and destruction should meet appropriate business or legal requirements and avoid unnecessary waste of computer resources. A copy of an email containing personal information about a WCDHB staff member or patient/client/consumer can be requested by that individual or their representative under the Privacy Act 1993 and the Health Information Privacy Code 1994. Government agencies often have legislative powers to request information held by WCDHB and this includes email. Email may also be subject to Police search warrants and used as evidence in Court. WCDHB staff should consider this when writing and sending email.

1.04 WCDHB staff members shall not:
   i) undertake any activity in support of charitable endeavours;
   ii) undertake any activity in support of a private or personal business enterprise;
   iii) send email messages which:
      a) may give offence to anyone who may or is likely to read them;
      b) inappropriately disclose confidential health or confidential WCDHB information;
      c) breach any statutory requirements;
      d) damage the professional image of WCDHB;
      e) make unauthorised public comment on official WCDHB matters or imply an official statement or opinion when authority has not been given to the author to do so;
      f) menace or harass any other individual.
   iv) intentionally Spam, or send Spam to, other WCDHB users.

1.05 Emails containing patient identifiable information may be sent via email providing:
   i) The destination address is one of:

- anyone@cdhb.govt.nz
- anyone@sissal.govt.nz
- anyone@cpublichealth.co.nz
- anyone@cph.co.nz
- anyone@healthfirst.govt.nz
- anyone@healthfirst.org.nz

ii) Or, the information is encrypted with a minimum of Advanced Encryption Standard (AES) 256 encryption rating before sending. Software to do this is available on all WCDHB computers.

1.06 All WCDHB staff are on one of 3 storage tiers - low, medium and high. Storage tiers have limits on how much email is permitted, before restricting the ability to send and/or receive emails. Staff are required to regularly archive emails before moving up to the next storage tier. The Information Technology department can enable email archiving by request.

1.07 The Information Technology Department, may with the prior approval of a General Manager, monitor Email use at any time. Monitoring may include reading email, and recording information on email sent and received, information downloaded to or transmitted from the WCDHB Network, and information transmitted or uploaded via email.

1.08 Users must discuss the transmission and reception of large attachment files, or multiple small attachment files, with the Information Technology Department. As a guideline, a large file is considered to be greater than 10 Megabytes (MB). With multiple files, it is the total size of all files that is considered, not individual sizes.

1.09 Any possible breaches of this Procedure are to be reviewed by the Manager – Information Technology and the Quality Assurance and Risk Manager to determine if a breach has actually occurred.

1.10 Where the Manager – Information Technology and the Quality Assurance and Risk Manager agree that a breach has occurred, then it is to be reported (as soon as practicable) to the relevant General Manager. (*For the purposes of Sections 1.07 and 1.08 the relevant General Manager is the General Manager who has responsibility for the Unit/Department/Service within which the computer on which the breach was detected is located*). Where the detected breach involves a General Manager, then this is to be reported to the Chief Executive Officer. Where the detected breach involves the Chief Executive Officer, then this is to be reported to the Chair of the Board.

1.11 All breaches detected are to be investigated at the discretion of the relevant General Manager/Chief Executive Officer/Chair in accordance with the WCDHB Staff Discipline Procedure.

7. Precautions and Considerations

➔ Email users must primarily use email for official WCDHB business

➔ Email users must not misuse email

➔ Access to the Email will be on the basis of identification and authentication of authorised users

8. References

There are no references associated with this Procedure.

9. Related Documents

WCDHB Access To Information Systems Procedure

WCDHB Internet Use Procedure

Revision History	Version:	7
	Developed By:	Information Technology Manager
	Authorised By:	Chief Executive Officer
	Date Authorised:	July 2001
	Date Last Reviewed:	June 2019
	Date Of Next Review:	June 2020