1. **Scope**

Every individual who uses organisational e-mail facilities is required to comply with what Retirement Capital considers to be the minimum standard required for the proper use of those facilities.

1. **Responsibilities**
   1. Every employee/member of staff, sub-contractor or temporary worker is responsible for not compromising Retirement Capital through the use of organisational e-mail facilities.
   2. The IT Manager is responsible for providing the required standard e-mail footer and for setting and monitoring mailbox size limits.
   3. The Training Manager is responsible for ensuring that all users of e-mail have been trained in this procedure.
   4. The Information Security Manager responds to and manages information security incidents and provides cryptographic controls in line with Control A.10 Cryptography (See Information Security Manual).

1. **Procedure** [ISO27002 Clause 8.1.3; 13.2.1; 13.2.3]
   1. Organisational e-mail facilities may not be used for sending defamatory e-mails, or using e-mail for harassment, unauthorised purchases, or for publishing views and opinions (defamatory or otherwise) about employees/staff, workers, suppliers, partners or customers of Retirement Capital.
   2. All e-mails have an automatic footer that contains the legal disclaimer set out in [ISMS-C DOC 8.2](ISMS-C_DOC_8.2.docx) and users are prohibited from amending or deleting it.
   3. Organisational e-mail may only be used for the communication of confidential information in line with the requirements of [ISMS-C DOC 8.2](ISMS-C_DOC_8.2.docx).
   4. Outgoing e-mail attachments must be appropriately protected, using (where required by control section 8.2.1 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)) cryptographic controls.
   5. Users must not open incoming e-mail attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party, were not expected. These attachments may contain viruses, worms or Trojans and any such e-mails must be reported to the Information Security Manager immediately, by telephone or in person, and on no account should they be forwarded, or copied on, to anyone, whether inside or outside the network.
   6. Viruses and hoax virus messages: users are required to report any third party e-mail messages they receive about viruses to the Information Security Manager immediately, by telephone or in person, and on no account should it be forwarded, or copied on, to anyone, whether inside or outside the network.
   7. Users are prohibited from using organisational e-mail facilities for forwarding chain letters or impersonating other people, nor may organisational e-mail addresses be left on any websites other than for legitimate and necessary business purposes.
   8. Users are required to limit the use of group e-mail addresses, to limit copying to unnecessary recipients, to restrict use of the ‘reply to all’ function, and restrict the use of the blind copying feature.
   9. Users are required to comply with the Incident Reporting Procedure referenced at control section 16 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx).
   10. Employees/staff are required to delete non-essential e-mail messages as soon as possible and, on a regular basis, to clear e-mail boxes of correspondence that is no longer required. The archive facility should be used so that messages that need to be retained but which are no longer current can be removed from the inbox. These controls are necessary so as to avoid e-mail boxes becoming so full that more and more server space is required to support the system. The sent items box must also be weeded on a regular basis. The IT Manager must ensure that maximum individual mailbox sizes are set which, after two early automated warnings, cannot be exceeded. The procedures for this are clearly documented in work instruction [ISMS-C DOC 8.1.3b](ISMS-C_DOC_8.1.3b.docx).
   11. Organisational e-mail may not be used to purchase anything on behalf of Retirement Capital without specific prior authorisation, and then only in accordance with Retirement Capital’s current policy on purchasing and cryptographic controls (see control section 10.1 of the [Manual](../Manual/001%20Information%20Security%20Manual.docx)).
   12. Organisational e-mail addresses may not be used for personal purchases or any other personal transactions.
   13. Employees/staff are prohibited from setting up automatic forwarding of e-mails to addresses external to Retirement Capital or of copying e-mails to addresses outside Retirement Capital unless there is a legitimate business purpose for doing so.
   14. Breaches of these requirements may be dealt with under Retirement Capital’s disciplinary policy as set out in the [Employee Handbook](../../../QEMS/08%20Employee%20Handbook%20(EH)/QEMS-EH-DOC-001%20Employee-Handbook%20v2%20-%20July%202019.pdf).

***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Chief Information Security Officer (CISO (DIRECTOR)) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |