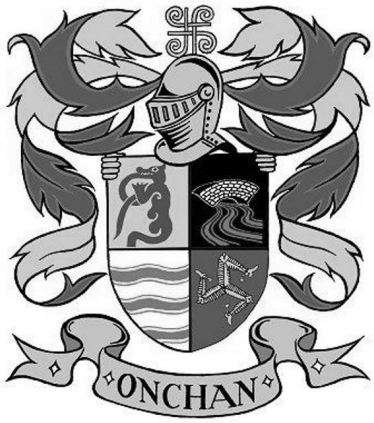

ONCHAN DISTRICT COMMISSIONERS

INTERNET AND EMAIL POLICY

Version 1.0

Adopted:
18th November 2013

Contents

Introduction

It is important that you read each section that affects you or your work since you will, in the future, be deemed to be aware of its contents in the event that there is any breach of the Authority's policy.

The Authority wishes to encourage the use of electronic media in the conduct of its business. The Authority expects you to use these facilities sensibly and act professionally as you would in the normal course of work. For example, when sending e-mail messages, you should always use the same safeguards and precautions as you would when sending a fax or letter. Similarly, you should exercise proper judgement as to which internet sites you visit.

The Authority accepts that it is sometimes difficult to be sure of the boundaries between what is acceptable and unacceptable behavior, and we have set down guidelines for the use of the Authority's IT system (which may be amended from time to time). If you do not understand any of the following rules, please discuss this with your manager.

Overview

The purpose of this policy is to describe the acceptable use of Onchan District Commissioners' email and related services, systems and facilities.

The Policy will be made available to users of the email and related services and facilities. There will also be periodic review of the Policy and amendment if necessary,. This will be with regard to the development of the system, the operational use of the system and generally recognised best practice.

Email access is provided by Onchan District Commissioners to support its role in respect of local authority services, research and associated functions related to this role.

Statement of Authority and Scope

This policy is intended to detail the rules of conduct for all personnel including Members of the Board of Onchan District Commissioners (the Authority) who use email and related services. This e-mail Policy applies to the sending or receiving email messages and attachments. The Policy is applicable to all members of the Commissioners including staff and other authorised users of the Authority's IT facilities.

Only authorised users of the Authority's computer systems are entitled to use email facilities. All members of the Authority who agree and abide by the Authority's regulations, are entitled to use computing facilities and email systems at all times when the network is available.

The Authority complies with and adheres to all its current legal responsibilities including Data Protection.

Statement of Responsibilities

Individual users are responsible for their own actions. The use of email facilities by individuals at Onchan District Commissioners assumes and implies compliance with this policy, without exception, and those Acts, Policies and Regulations enacted or authorised by the Authority or other regulatory bodies. Every user of email systems has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard.

The Chief Executive will be responsible for ensuring that the Managers are aware of this policy; and they in turn will be responsible for informing their people of this policy.

The I.T. Contractor is responsible for providing and maintaining central email systems.

Onchan District Commissioners are responsible for email policy as a whole. Within each Department, certain areas of IT and computer security will be delegated to local support.

Acceptable Use

1. General

The Authority's main purpose in providing IT facilities for email and the internet is to support the approved business activities of Onchan District Commissioners. IT facilities provided by the Authority for internet and email should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- Creation or transmission of material which brings Onchan District Commissioners into disrepute.
- Creation or transmission of material that is illegal.
- The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind
- The unauthorised transmission to a third party of confidential material concerning the activities of Onchan District Commissioners.
- The transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users.
- Activities that corrupt or destroy other users' data or disrupt the work of other users.
- Unreasonable or excessive personal use. (See 2 below).
- Creation or transmission of any offensive, obscene or indecent images, data or other material. (Other than for reasons specified in 3 below).
- Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or anxiety.
- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, and disability, political or religious beliefs.
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature.

- Activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals.
- Creation or transmission of anonymous messages or deliberately forging messages or email header information, (ie without clear identification of the sender) or for 'flaming'.
- The unauthorised provision of access to Onchan District Commissioners' services and facilities by third parties.

2. Personal Use

We appreciate that you may occasionally want to use the system and/or the facilities for your own purposes and we expect you to use it responsibly. If at all possible, make it clear that you are representing yourself in a personal capacity. For example, indicate that the e-mail is personal/not work related. Always follow the rules and guidance set out in the internet and e-mail policies and, particularly, ensure that your personal use of the system:

- ♦ does not take priority over your work responsibilities;
- ♦ does not incur any unwarranted expenses on the Authority; and
- ♦ does not have a negative impact on the Authority in any way.

An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):

- A level of use that is not detrimental to the main purpose for which the facilities are provided. *Priority must be given to use of resources for the main purpose for which they are provided.*
- Not being of a commercial or profit-making nature, or for any other form of personal financial gain.
- Not be of a nature that competes with Onchan District Commissioners in business.
- Not be connected with any use or application that conflicts with an employee's obligations to Onchan District Commissioners as their employer.
- Not be against Onchan District Commissioners' rules, regulations, policies and procedures and in particular this email policy.

3. Research and Related

It is recognised that, in the course of their work or research, individuals of the Authority may have a requirement to transmit or receive material that would normally be defined as offensive, obscene, indecent or similar. In the case of properly supervised or lawful research purposes it is acceptable to do so. If in doubt advice should be sought.

Use of Email

Care should be taken when using e-mail because e-mail messages are perceived to be less formal than paper-based communication and there is a tendency to be lax about their content. Bear in mind that all expressions of fact, intention and opinion via e-mail can be held against you and/or the Authority in the same way as verbal and written expressions or statements. Do not include anything in an e-mail which you cannot or are not prepared to account for. It is good practice to re-read each e-mail in hard copy before sending it; an e-mail cannot be retrieved once it is dispatched.

E-mail messages which have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending e-mail can be identified. E-mails, both in hard copy and electronic form, are admissible in a court of law.

If your e-mail message is confidential, ensure that the recipient is comfortable with this means of communication. Further, be aware that other persons may have access to the recipient's messages. If the content is highly confidential, you should perhaps consider other more traditional but secure means of communication.

Your e-mail should always include a signature and the Authority's confidentiality notice.

If you encrypt or scramble any e-mail or other document, you must ensure that your line manager is given:

- details as to each country to or from which an encrypted communication is intended to be sent or received,
- a complete and up-to-date copy of any private, public or other decryption key, and
- all other information required for the efficient decryption of the relevant document.

Confidentiality

All information relating to our customers, tenants, staff and the business operation of the Authority is confidential. You are expected to treat electronic information with the same care as you would paper-based information which is confidential. Keep all such information secure, use it only for the purpose(s) intended and do not disclose the same to any unauthorised third party (which may sometimes include other employees of the Authority).

- Keep your passwords safe. Do not disclose them to anyone (save as required to enter onto the register). It is advisable to change your passwords from time to time for security reasons. A register of passwords will be kept in secure storage by the Chief Executive and all passwords must be recorded therein.
- If a document is highly confidential or sensitive in nature, you should store it in a private directory or an equivalent password protected directory. When deleting such documents, ensure that you empty your recycle bin well. Bear in mind that most documents can be accessed by all employees in the Authority.
- Copies of confidential information should only be printed out as necessary (and retrieved from the printer immediately) and stored or destroyed in an appropriate manner.

Intellectual Property

Broadly speaking, intellectual property refers to copyright material, designs, patents, trade marks, inventions, ideas, know-how, business information and lists. Most images, text and materials are protected by copyright; others are protected by trade marks. The downloading, possession, distribution or copying of a copyright work, for example a document, photograph, piece of music or video, is an infringement of copyright unless the person downloading is properly authorised to do so by the copyright owner. These basic principles also apply to materials obtained from third parties such as customers, other companies, information services and internet sites. If you have any enquiries or concerns, speak to your line manager, Finance Manager or Deputy Clerk.

Ownership

All intellectual property created in the course of employment belongs to the Authority. All computer equipment, software and facilities used by you are also proprietary to the Authority, including all documents, materials and e-mail created. Accordingly, you should use the Authority's property and intellectual property only in the work context and solely for the benefit of the Authority, subject to the modest personal use permitted in 2 above.

The Authority reserves the right to monitor, access, retrieve, review and delete the following without notifying the individual concerned:-

- all e-mail sent, received or in the course of composition;
- mail boxes and private directories;
- all use of the internet and all other communication techniques deployed by you using the system; and
- any third party screen savers, software, materials, etc. on the system.

The Authority also reserves the right to withdraw any of the facilities provided if it considers that your use of it is in any way unacceptable.

Quotas and Limits

All users have access to the centrally-managed email server. All accounts have quota limits placed on them. All file partitions are backed up to tape on a regular basis. Accounts that are removed will have their files archived. Unless specifically requested no archiving takes place.

Virus Checking

Computer viruses, trojans and worms are collectively known as malware. One common method of distributing malware is via email. All email communication through the Authority's email gateways is checked for malware. Checking strategies include: refusing messages containing executable attachments or zip files, scanning messages for known malware or a combination of both techniques. Please note that this is a separate procedure and not related to the virus scanning policy applied to the central fileserver.

Messages containing malware will be retained for up to a month for administrative reasons. The **sender** of such messages will be informed of the viral content of their email. A similar message will be sent to the administrator(s) of the email gateways.

Virus check all material which is down loaded from the internet or received from any external source.

Automatic email forwarding

Automatic forwarding or redirection of email to other mail domains is possible. Onchan District Commissioners will not be responsible for email forwarded off the network. It is the individual's responsibility to set forwarding policies up and to make sure the forwarding address is correct and the email service being used is reputable and reliable. Users must exercise caution when automatically forwarding any email to an outside network and question the need to do so. All our email services are accessible to authorised users from the Internet.

Allowing other people to access email can be achieved directly by sharing email folders and mailboxes.

Logging

Traffic through the Onchan District Commissioners email gateways is logged. Logs include details of the flow of email but **not** the email content. Transaction logs are kept online for up to a month. Backups of these logs are kept for up to 3 months. Logs are available to authorised systems personnel for diagnostic and accounting reasons.

Standards

The Onchan District Commissioners email gateways will attempt to verify the source and destination of email before being passed on.

Spam and Junk Mail

Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming. In reality spam and junk mail are regarded as interlinked problems.

A certain amount of junk mail is blocked at the mail gateways.

Incoming email is also checked against and there are methods individuals can use to filter this email.

Remote Access

Remote access to Onchan District Commissioners email servers (for reading email) is possible via the Internet. Any Officer or Member wishing to use this facility should discuss the matter with the Chief Executive or Finance Manager.

Incident handling and data protection

Onchan District Commissioners will investigate complaints received from both internal and external sources about any unacceptable use of email or IT facilities. The Chief Executive, in conjunction with other departments as appropriate, will be responsible for the collation of information from a technical perspective. It should be noted that logs are only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended.

Where there is evidence of a breach of this policy it will be investigated in accordance with Onchan District Commissioners disciplinary procedures applicable to all members of staff. In such cases the Chief Executive will act immediately with the priority of preventing any possible continuation of the incident. That is, accounts may be closed or email may be blocked to prevent further damage or similar occurring.

Data Protection

The Authority holds and processes personal data and has responsibilities under the Data Protection Act 2002 (“the Act”). All employees have an obligation to assist the Authority in complying with its responsibilities under the Act and you should exercise due care when holding, processing or disclosing any personal data.

An individual is able to make a Data Subject Access Request for any personal information held by an organisation on that individual. This request not only applies to information held on computer, including emails, but also to CCTV images and manual files, provided they are held in a "relevant filing system".

A typical example of a relevant filing system is Personnel Records; access to these records would include access to any confidential references that have been received and form part of that file.

A subject access request applies to all personal data held in a relevant filing system. It does not matter how "old" the data is; if the data is held in a relevant filing system then the data can be accessed.

A data controller has 40 calendar days to comply with such a request.

If the Data Controller fails to comply with the request, then the individual may:

- Apply to the Court and the Court may, not only, order compliance with the request, but also, impose a fine up to £5,000.
- The individual may also seek compensation for distress alone if the failure to comply with the request was unjustified.
- Request the Data Protection Supervisor to undertake an assessment

Local Authorities are data controllers and are not exempt from prosecution.

Disciplinary action

If you ignore the rules and guidance set out above or misuse and/or abuse the system, its facilities or any property belonging to the Authority, you will be liable to disciplinary action. It may also lead to summary dismissal. The Authority will take any breach of these rules very seriously. At the same time, your conduct and/or action(s) may be unlawful or illegal and you may be personally liable.

If you are unclear about any of the issues discussed in this policy, please speak to your line manager, Finance Manager or Deputy Clerk – always ask before acting.