


Policy No: 03-1508	Authorised: 	Date: 04/02/2020
<b>ELECTRONIC COMMUNICATIONS POLICY CODE OF PRACTICE</b>		

*This Policy sets out a Code of Practice which describes the key elements to be addressed and guidelines to be followed to ensure that all of the Organisation's electronic communication systems are used effectively, efficiently, safely and securely:*

## CODE OF PRACTICE:

### 1. USERNAMES:

Users are responsible for all actions taken using any computer name assigned to them. It is essential that usernames are not abused in any way, and that username management is restricted to the following:

- 1.1 Ensuring proper password protection for the unique username;
- 1.2 Restricting usage to authorised personnel only; i.e. not allowing anyone else to use the username;
- 1.3 Not using someone else's username;
- 1.4 Not abusing the privileges granted to the username;
- 1.5 Not keeping a paper record of usernames.

### 2. PASSWORDS:


Password provide a key method of validating a user's identity, and therefore the authority to access an information system or service if the appropriate access rights have been given. The following guidelines should be adopted for every password user:

- 2.1 Passwords should be made up of a minimum of 7 characters, at least 2 of which must be numerical;
- 2.2 Do not keep a paper record of passwords;
- 2.3 Passwords should be kept confidential;
- 2.4 Passwords for individual usernames should not be shared;
- 2.5 Passwords should be changed monthly.

### 3. ELECTRONIC MAIL (e-mails):

The Organisation provides e-mail facilities for users, and those who use e-mail services are expected to do so responsibly by complying with Organisational policy and applicable laws. *It must be remembered that all laws governing copyright, defamation, discrimination, data protection, and all other laws which apply to other forms of written communication also apply to e-mail.* In particular, e-mail users MUST NOT:

- 3.1 Use the e-mail system to directly or indirectly interfere with the Organisation's operation of its computer facilities or e-mail systems;
- 3.2 Allow the use of e-mail to interfere with the e-mail user's employment obligations to the Organisation;
- 3.3 Set auto-forwards to external e-mail accounts;

Policy No: 03-1508	Authorised: 	Date: 04/02/2020
<b>ELECTRONIC COMMUNICATIONS POLICY CODE OF PRACTICE</b>		


- 3.4 Use e-mail for any other employment or business activities;
- 3.5 Send e-mail from other people's accounts unless specifically authorised to do so by the account holder;
- 3.6 Attempt to read, modify or delete e-mail which is not addressed to you, unless specifically authorised to do so by the account holder;
- 3.7 e-mail the Organisation's confidential information unless it is encrypted;
- 3.8 Use e-mail as a means of harassment, (racial, sexual or otherwise);
- 3.9 Make defamatory statements in any e-mail, and / or circulate material that could be deemed to be illegal, offensive, obscene, racially intolerant, or antisocial;
- 3.10 Circulate unlicensed material protected by third party intellectual property;
- 3.11 Circulate games, jokes, cartoons, movie clips, images etc unless required for business purposes;
- 3.12 Send e-mail chain letters;
- 3.13 Send replies to "all recipients" unless there is a very specific need for everyone to receive the message – it wastes disk space and clutters up in-boxes.

#### 4. INTERNET:

The Organisation has provided corporate gateways for internal access which will allow a variety of incoming and outgoing services while maintaining an acceptable level of security.

Inappropriate use of the internet may be subject to formal disciplinary action. Examples of inappropriate use will include, but are not limited to, the following:

- 4.1 Access for private gain or non-Company commercial purposes;
- 4.2 Deliberate use of the internet for social networking, and for accessing chat-lines and material of a pornographic, hateful, obscene, racist or otherwise illegal nature;
- 4.3 Access for political lobbying;
- 4.4 Downloading copyrighted software and material without compliance with, and in violation of, all terms of the authorised licensing agreement;
- 4.5 Placing copyrighted material on any part of a web page without full compliance with the terms of the copyright.
- 4.6 Using the computer to perpetrate any form of fraud, or software, film or music piracy.

Policy No: 03-1508	Authorised: 	Date: 04/02/2020
<b>ELECTRONIC COMMUNICATIONS POLICY CODE OF PRACTICE</b>		

- 4.7 Hacking into unauthorised areas.
- 4.8 Introducing any form of malicious software into the computer system.
- 4.9 Revealing any form of confidential information about the Organisation, to include financial information, and information about clients, policies, business plans, staff and the content of internal memoranda and / or discussions.


#### 5. VIRUS PROTECTION:

The Organisation has installed a firewall and virus protection programme on its computers and servers to minimise infection and the spread of viruses. However, with new viruses appearing on a regular basis it means that occasionally documents may be sent to the Organisation that are infected with a virus which remains undetected and may pass through a firewall. The following actions should therefore be taken to minimise the risk of virus infection:

- 5.1 Ensure that your workstation has anti-virus software installed, and that this is up-dated on a regular basis.
- 5.2 Ensure that all software comes from reputable sources, and avoid Shareware, free "catalogue" disks and games.
- 5.3 Do not open e-mail attachments unless you are absolutely sure of the authenticity of their origin;
- 5.4 When reading e-mail attachments do not enable Macros as a matter of course;
- 5.5 Report all suspected virus incidents to the Help Desk or through the intranet.

#### 6. SOFTWARE COPYRIGHT:

- 6.1 The Organisation has a legal obligation to comply with all copyright restrictions on software installed on its IT systems, and such restrictions are generally detailed in Software Licenses.
- 6.2 Copyrighted software must only be used in accordance with its license or purchase agreement, and must not be copied or altered except as permitted by law or by the software Licensing Agreement.
- 6.3 Unauthorised copying, distribution, or use of such software is a crime and the Organisation as well as individuals may be held legally liable for these actions. Any user who breaches license conditions may face disciplinary action and / or prosecution under the *Copyright, Designs and Patents Act, 1998*, and the *Copyrights and Rights in Databases Regulations, 1997*.

Policy No: 03-1508	Authorised: 	Date: 04/02/2020
<b>ELECTRONIC COMMUNICATIONS POLICY</b> <b>CODE OF PRACTICE</b>		

**FORMS REFERENCES:**

*Risk Assessment - Electronic Communications*