Email and Internet Acceptable Usage Policy

**Introduction**

Every employee has a responsibility to maintain the company’s image, to use these electronic resources in a productive manner and to avoid placing the company at risk of legal liability based on their use.

**Scope**

This policy applies to allemployees when using the Internet in and/or electronic mail in COMPANY.

**Principles**

COMPANY’s Internet connections are intended for activities that either support COMPANY’s business or the professional development of employees. System users are expected to be responsible, considerate and ethical in using company systems, to protect valuable company information and to exercise prudent judgement. Misuse of company systems may result in restriction or termination of access privileges and other disciplinary action, up to and including termination.

All messages distributed via the company’s email system, even personal emails, are COMPANY’s property.

Internet usage or emails can be monitored without prior notification if COMPANY deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the company reserves the right to take disciplinary action, including dismissal in line with the company Disciplinary policy and/or legal action where appropriate.

The below outlines the standards that employees are held to in relation to the usage of company internet and email systems. The policy follows the Data Protection Commissioners published guidelines and is in accordance with the Data Protection Acts 1998-2018.

**1 –Potentially dangerous material**

Do not launch, detach or save any executable file under any circumstances. If you receive any material which you believe has the potential to be dangerous or damaging you must contact IT Division immediately.

All incoming attachments must be virus checked by IT Division. Please note that all portable storage devices (e.g. USB sticks) brought into the office from home PC's should also be virus checked by IT. The safer option is to forward these attachments by e-mail from your home PC as they will be automatically screened by the company’s anti-virus software.

Do not open, detach or save any unofficial file attachments to any network drive. Official attachments should be placed in the relevant document Library or detached to a shared drive. Please beware of saving any documentation to the hard drive of your PC as this will not be backed up and will be irretrievable in the event of your PC breaking down.

**2. Obscenity, Child pornography and Incitement to hate.**

You are subject to all legislation regulating Internet use, including the provisions regarding obscenity, child pornography, sedition and the incitement of hate. In particular, persons have obligations under the Irish Child Trafficking and Pornography Act 1998, not to allow any of its systems (mail, Internet etc.) to be used for downloading or distributing offensive material.

**3. Other Offensive and Time wasting Material**

Unsolicited material can arrive from anywhere. Should you receive material which you find offensive or abusive or time wasting respond notify your manager and/or Human Resources.

In the case of any Spam mail don't issue any reply.

**4. Misleading information**

Always be aware that the Internet is an unregulated, world-wide environment. It contains information and opinions that range in scope from reliable and authoritative to controversial and extremely offensive. It is your responsibility to assess the validity of the information found on the Internet.

**Material you send**

Remember that e-mail is effectively on official headed paper and can be traced back to place, date and time of sending. Make sure you are satisfied with its content and that it has been approved at the appropriate level. Double check the address of the intended recipient. Once the "send" key is pressed, e-mail cannot be stopped or retrieved. Deleting mail from your system does not make it untraceable.

Do not send any unofficial graphics or executable files under any circumstances. Do not instigate or forward "unofficial mail" to users either within or outside the Office or send any material which may be offensive or disruptive to others or which may be construed as harassment. Do not make derogatory comment regarding gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of the travelling community.

Remember that screensavers can be a means of causing offence.

Do not use another employee's e-mail account.

All e-mails are automatically backed up and are recoverable.

**Screening procedures**

The Company’s IT screening system will automatically screen all mail for known viruses, attachments etc.

IT does not normally read individuals mail or open mail boxes except:

(1) where the screening software or a complaint from an individual indicates that a mailbox contains material which is dangerous or offensive.

(2) where a legitimate work reason exists to open the e-mail.

Opening mailboxes for investigation requires authorisation by Senior management on a case by case basis. The individual's mailbox, hard disk, network drive and relevant backups are then searched.

Where investigation proves that a problem exists it will be reported to the sender, their organisation, the staff member concerned, Head of Division and/or HR Manager for appropriate action. Where the problem concerns material such as a virus or an unauthorised .exe file, which can damage the network, IT may immediately close down an account pending further investigation and action.

Messages containing virus files are not retained.

**Time wasting and resources**

Network resources such as storage space and capacity to carry traffic are not unlimited. However your time and that of your colleagues is the most valuable resource available to the Office.

You must not deliberately perform acts which waste your own and your colleagues time or computer resources. These acts include

* Playing games
* Online chat groups
* Uploading / Downloading large unofficial files which create unnecessary non-business related loads on network traffic
* Accessing streaming audio / video files, for example, listening to music or watching movie clips
* Forwarding audio / video files to colleagues
* Participating in mass non-business related mailings such as chain letters
* Sending unofficial attachments

**Financial Implications**

Do not download any material / software from the Internet for which a registration fee is charged without first obtaining the express permission of the Office. Only the software installed by IT Division, and therefore listed on the Offices Assets Register, is deemed to be legally sourced by the Office and covered by the appropriate licence agreement. No other software is approved for use on any of the Offices computers or laptops.

**Security**

You are responsible for the use of the facilities granted in your name. The main protection at present is your password. Make it difficult to guess and above all, do not share your password with anyone, write it down or give it out over the phone. If you think someone knows your password, ask for it to be changed as soon as possible. Maintaining the privacy of your password is your responsibility and consequently you are responsible for any abuses taking place using your name and password.

In general do not leave your computer unattended without securing the session by password or signing off.

When leaving your pc unattended press Ctrl Alt Del (in the same way as logging into your pc) and click the "Lock workstation / Lock computer" box. On return press Ctrl Alt Del and enter your password to log back into the pc.

Users accessing the Internet through a computer attached to the Office's network must do so through an approved Internet firewall or other security device. Bypassing the Office's computer network security by accessing the Internet directly by modem or other means is strictly prohibited.

You are reminded that files obtained from sources outside the Office, including files downloaded from the Internet, news groups, bulletin boards or other online services and files attached to e-mail messages may contain computer viruses that may damage the Office's computer network. While the Office is continually upgrading its virus protection infrastructure, the potential introduction of viruses on the Office system always remains a threat. All incoming material, regardless of origin, should be virus checked before being used on any PC on the Office's network.

The Internet is not secure. Whether by e-mail or via the World Wide web, do not give out more information than is necessary to fulfil your purpose. Beware of demands for unnecessary information. Be wary of sites which request more data than is necessary for accessing the site or for making a transaction, or which do not tell you why they require this data from you. In particular, no information on IT systems or resources should be disclosed over the Internet or through e-mail without authorisation from IT Division.

External e-mail should only be used to transmit unclassified information to individuals outside the Office. Classified or confidential material should not be sent by e-mail unless it is encrypted.

**Web Logs**

All web browsing is logged. Screening software prevents access to certain non-work related sites. The logs of web browsing will only be accessed with management authorisation, where there are reasonable grounds to believe that this policy has been contravened.

**Personal Use**

Just as with the phone, a small amount of limited personal use of e-mail and Internet facilities is permitted if such use does not otherwise infringe this policy.

**Freedom of Information and Archives Acts (only applies to public bodies)**

Incoming and outgoing e-mail's which are of "enduring organisational interest" are records under the above Acts and must not be kept in your e-mail account. They must be transferred to the appropriate document library or file.