Policy for ICT Acceptable Use

Institute for Optimum Nutrition

1. Scope of policy

1.1 This policy applies to all members of staff, contractors or individuals who have reason to access Institute for Optimum Nutrition systems primarily provided for members of staff.

2. Policy

1.1 The Institute relies on its computer and communications facilities to carry out its business. All these facilities can be put at risk through improper or ill-informed use, and result in consequences which may be damaging to individuals and their research, the Institute community and to reputations.

1.2 The policy aims to provide clear guidance to all employees concerning the use of Institute computer and communications facilities. It provides a framework to

- enable employees to use Institute facilities with security and confidence,
- help maintain the security, integrity and performance of Institute ICT systems;
- minimise both the Institute and individual users' exposure to possible legal action arising from unauthorised use of the ICT systems;
- set the minimum standard for acceptable use across all Institute ICT systems.

1.3 It is the Institute's responsibility to ensure that employees have access to this policy, both on joining and during their employment. It is each employee's responsibility to read, make themselves fully familiar with, and abide by the policy, and any relevant local policies.

1.4 The policy covers use of all ICT systems and facilities provided either directly or indirectly by the Institutes or used to conduct Institute business, whether accessed from an Institute site or remotely, in particular:

- Electronic communications (in all forms) for example e-mail, social media used for business related communication, etc.
- electronic bulletin boards and social media

- file sharing by whatever means
- Computing devices (e.g. Desktops, laptops, printers, mobile devices etc.) and servers
- Communications equipment (e.g. telephones (land-line and mobiles), faxes and video conferencing)

1.5 Sensitive or personal information must be appropriately protected in line with the **Policy for Data Protection and Processing**.

1.6 Any activity that falls outside acceptable use (see Appendix A) may result in disciplinary action (see the **Employee Handbook**). Where the activity is deemed to amount to gross misconduct, this will normally lead to summary dismissal. For non-employees any action will be discussed with the individual's management (as appropriate); this may include being denied access to Institute/establishment sites. Any suspected illegal action will be reported to the police.

1.7 Non-employees will be made aware of the principles of the Policy, and any restrictions/guidance, before they have access to Institute ICT systems and services. This will include a statement on private/personal use (which should be in line with the restrictions placed on Institute staff but may be more restrictive if required).

Monitoring

1.8 Monitoring Statement

2.1.1 The Institute reserves the right to monitor communications.

2.1.2 The Institute employs monitoring techniques on its ICT systems and services, including e-mail and Internet access, to enable usage trends to be identified and to ensure that these facilities are not being misused.

2.1.3 Monitoring is limited, as far as practicable, to the recording and analysis of network traffic data. To this end, the Institute keeps logs of: calls made on communications equipment such as telephones and fax machine; emails sent by e-mail address; internet sites visited by computer system address. In some cases, this means that the identity of the individuals involved in the communication is readily available. These logs are not routinely monitored on a continuous basis but spot-checks are carried out from time to time to help ensure compliance with this policy. Further authorised investigations may be necessary where there is reasonable suspicion of misuse of facilities.

2.1.4 Since the Institute owns and is liable for data held on its communications equipment and systems, it reserves the right, as part of any investigations, to inspect the contents of any e-mails or any other form of communications that are sent or received and of Internet sites accessed, for compliance with this policy. This will only be done where the volume of traffic or the amount of material being downloaded is excessive, or there are grounds to suspect that use is for 'unacceptable' or 'forbidden' activities (see examples in Appendix A).

2.1.5 Exceptionally, where there is a defined and valid reason for doing so, the inspection may include items marked 'private' or 'personal'. An individual's e-mail and voice-mail accounts may also be accessed by management when the individual is absent from work to ensure

official business matters can be effectively dealt with. Authorisation for such access is given by the Senior Management Team. Management will make a reasonable attempt to inform and obtain agreement from the user prior to this occurring.

2.1.6 Monitoring/investigations of individuals' use of the Institute's communications systems may also happen in the following circumstances:

- To detect or prevent crime including detecting unauthorised use of systems, protecting against viruses and hackers and fraud investigation
- To assist in maintaining the security, performance, integrity and availability of the ICT systems, services and facilities.
- To provide evidence e.g. of a commercial transaction, to establish regulatory compliance, audit, debt recovery, dispute resolution.

2.1.7 Where monitoring is used, only Institute staff trained in data protection compliance will investigate the recorded data. Confidentiality will be ensured for all investigations involving personal data, except to the extent that wider disclosure is required to follow up breaches, to comply with court orders or to facilitate criminal investigation. Logged data will not normally be retained for more than one year unless required by regulatory compliance Please refer to the Institute **Policy for Data Protection and Processing**.

2.1.8 In addition, members of the IT Service Desk, will conduct random audits on the security of the Institute's ICT systems. These audits include examination of a small, randomly selected set of user devices and server systems. The audit checks that these systems have correctly licensed software, do not contain inappropriate material and have not been used to access or view inappropriate material that may violate this Policy.

2.1.9 Where monitoring reveals instances of suspected misuse of the ICT systems (e.g. where pornography or other inappropriate material is found, or where substantial time-wasting or other unacceptable/forbidden use is found), these will be investigated through normal disciplinary procedures and may result in dismissal.

2.2 Personal files, documents and e-mails

2.2.1 To help safeguard their privacy it is suggested that employees mark any personal e-mails they send with the word 'Private' in the "subject" line and to ask those they correspond with to similarly mark any personal e-mails being sent.

2.2.2 Personal files, documents and e-mails can be stored in ICT systems provided they are in a folder clearly marked as 'Personal' or 'Private'. Note that corporate electronic document or record management facilities (ERMS etc.) do not include a facility for personal data so should not be used for this.

2.2.3 Where possible, those staff responsible for monitoring or inspecting the IT and communications systems will respect e-mails and folders which are marked 'Personal' or 'Private'.

2.2.4 In cases where misuse is suspected, all appropriate ICT systems, including emails and folders marked 'Personal' or 'Private', will be checked to establish whether there may be a case to answer.

Private/Personal use of ICT systems, services and facilities

1.9 At management discretion, Institute employees are allowed reasonable personal use of Institute ICT systems, services and facilities provided that such use does not:

- interfere with their (or others') work; and/or
- involve more than minimal amounts of working time;
- incur any significant expense for the Institute and/or tie up a significant amount of resource.

1.10 Personal use should be limited to non-working time e.g. at lunchtime, before/after normal working hours. Limited, occasional personal use during normal working time will be tolerated (e.g. to respond briefly to an incoming personal e-mail or telephone call or to deal with a non-work related emergency). However, spending significant amounts of time making personal use of the internet, e-mail, communication equipment, etc. is not acceptable and may lead to disciplinary action.

1.11 Before undertaking personal use, employees should ask themselves the following questions.

- Would the actions be considered unacceptable if viewed by a member of the public?
- Would managers, auditors or others in similar positions call into question the cost effectiveness of use of work time or use of the Institute ICT systems and facilities?
- Will personal use have a negative impact upon the work of colleagues (e.g. in terms of their motivation and morale)?
- Could personal use bring the Institute directly or indirectly into disrepute?

Personal use should not be undertaken if the answer to any of these questions is yes.

1.12 Responsibility for ensuring that any personal use is acceptable rests with the individual. Employees should seek guidance from their line manager if they have any doubts concerning the acceptability of their personal use. If any doubt still remains, then that form of personal use should not be undertaken.

2. Social Media

2.1 The Institute recognises the value of using social media in work related communication. It can be an effective way to respond to queries, keep stakeholders informed, and track and respond to mentions of the Institute. Employees should have line manager approval before using social media for work related communication and must read and comply with any local rules before using social media for Institute related work.

APPENDIX A

Unacceptable Activities and Penalties

This policy sets the common minimum standards for the acceptable use of ICT systems and services. Set out below are examples of activities and uses which are specifically excluded.

The list is not comprehensive and is divided into two sections ("Unacceptable" and "Forbidden") to help highlight the most serious activities. The consequences of undertaking any of the activities listed below (or other instances) will be determined through the normal disciplinary procedures. All such activities are considered to be serious and are likely to be viewed as misconduct. It is likely that undertaking a forbidden activity, or repeating an unacceptable activity, will be viewed as gross misconduct.

Unsolicited receipt of discriminatory, abusive, pornographic, obscene, illegal, offensive or defamatory messages (e.g. email SPAM/text messages) will not be treated as a disciplinary offence. With the exception of illegal material, anyone who receives such material should follow local guidance on how to report it to the appropriate person. An employee who accidentally accesses a pornographic or other inappropriate web page should report the matter to their line manager. No disciplinary action will be taken in such cases. If the line manager is unavailable, the employee should contact the Business Manager.

Anyone accidentally viewing what they believe is illegal material (e.g. child pornography) must immediately stop what they are doing, take a note of where they found the illegal material and close the software application displaying the material; this includes email. The individual must not view the illegal material again and must take appropriate measures to ensure that others cannot view the material. They must inform their line manager and the relevant Business Manager, who will decide how to proceed. It may be a criminal offence to continue to view, allow others to view, or not to report some illegal material.

Examples of Unacceptable Activities

- Spending more than permitted amounts of working time making personal use of the internet, e-mail, and other ICT Systems and services.
- Transmitting, downloading or storing any material such that this infringes the copyright of the owner.
- Purchasing goods or services or entering into any contract via the Internet or any other ICT system on behalf of the Institute without the necessary authority.
- Business advertisements or trade sales*.
- Trading, i.e. sale of any goods purchased with the sole intention of making a profit*.
- Using an unauthorised electronic communication mechanism or cloud based service.
- Using unauthorised external email accounts for Institute businesses.
- Unauthorised redistribution of email.
- Sending or forwarding chain emails.
- Making your personal user name and password (also known as a 'user account') available for other people to use on your behalf.
- Accessing another individual's data, ICT systems or service without appropriate authorisation.

- Deliberately creating, storing or transmitting information which infringes the data protection registration of the Institute.