IT Acceptable Use policy

Approving committee:	Information Governance Committee
Minute reference:	IGC/07/12/2
Document owner:	Information Technology - IT Security
Key Contact(s):	Jeremy Harrington;
Date of Equality Impact Assessment:	06/07/2011
Equality Impact Assessment Outcome:	No impact
Latest review date:	22/01/2017
Next review date:	30/11/2018

1. Objectives and scope

The objective of this policy is to define and regulate acceptable use of Information Technology by Institute staff, students and visiting workers. This policy is mandatory and applies to all Institute sites as well as remote workers. It covers all Information Technology services including but not limited to Internet, e-mail, and instant messaging. This policy applies regardless of the particular technology, application or service used.

2. General policy

Information Technology facilities and services provided by the Institute are provided primarily for the purposes of cancer research and education as well as related supporting services. It is Institute policy that any such use must be lawful, must not expose the Institute or its staff or students to excessive risk or bring the Institute into disrepute. The Institute shall implement such lawful technical mechanisms as necessary to implement this policy.

3. Monitoring

The Institute reserves the right, conferred under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, to monitor staff and student electronic communications in exceptional circumstances with approval from the Directors of HR and IT to assure compliance with law and with policy, and continued effective operation of IT services.

4. Consent

ICR staff, students and visiting workers who use the Institute's IT facilities and services consent to abide by the terms of this policy.

4.1 Access to Individual Workspaces

In exceptional circumstances, a manager may need to gain access to work related information held on a user's workspace (e.g. the disk drive on an ICR computer used by them, their personal network area or M: drive, or their individual ICR email account). If contact with the individual is not practical and there is no other reasonably available source of the material, then, with approval from the Head of Division,

Corporate Director or their nominated deputies the appropriate IT staff will assist the manager to access the material. Reasons for this may include unscheduled staff absence from the office or other operational necessity. Personal material identifiable as such will not be looked at unless it relates directly to the material required.

Where a staff member has left the employment of the ICR, the same may also apply. However managers should always ensure that work-related information and emails are made accessible before staff and students leave.

Access may also be required where there is a reasonable belief that material held is required to assist an investigation under ICR policy or at the request of an external agency including audit, and cannot be otherwise obtained. In such cases, the agreement of both the HR Director and the IT Director is required.

4.2 Cookies

ICR's websites and web applications may use cookies for web analytics services. Cookies, which are text files, are placed on your computer for the purpose of evaluating the use of ICR websites and web applications in order for us to provide a better user experience.

The information generated by the cookie about your use of the ICR's websites and web applications is transmitted to and stored by ICR on our servers. This includes your IP address. This is not associated with your personal data held by ICR. We may also transfer this information to third parties where required to do so by law, or where such third parties process the information on ICR's behalf. This may include the transfer of information to a third party outside the EEA.

5. Allowed personal use

Limited and reasonable personal use of Institute's IT services is allowed in accordance with Institute policies provided it is legal, does not and is not seen to be bringing the Institute into disrepute, and does not affect the job responsibilities of the individual in particular or the mission and objectives of the Institute in general. In the first instance "reasonable use" is to be determined and communicated by line managers having due regard to legitimate expectations of staff and students and the interests of the Institute. Any disputes between individuals and their line managers are to be handled in accordance with the relevant Institute policies.

Such constraints on allowed personal use will include use of the web, social networking sites, video or music sites, or other Internet sites. Such personal use should not be conducted in areas open to or viewable by the general public, patients or visitors to the Institute.

6. Explicitly forbidden use

The following activities or uses of Institute IT facilities and services are forbidden and should be promptly reported to the HR Director for investigation. Where management has reasonable cause to suspect illegality, the matter should be treated as an Information Security incident, and the Policy for Information Security Incidents and Computer Forensics Management invoked.

a. Illegal activities

i. Any activities that are illegal under UK law, including but not limited to activities related to terrorism, child pornography, or incitement to violence. The Institute is also legally obliged to adhere to provisions of the Statutory Duty to Prevent. This list is not exhaustive and it is individuals' responsibility to ensure

compliance with applicable laws. In most serious cases (e.g. terrorism, child pornography) the Institute and its officers have legal obligations to report reasonable suspicions to the police.

ii. Creation or distribution of libellous or defamatory messages or

statements concerning any individual.

iii. Creation, access to or distribution of obscene, indecent, bullying, harassing or grossly offensive material.

iv. Creation or distribution of any malicious computer code, scripts or

code intended to affect computer operations contrary to provisions of the Computer Misuse Act as amended.

v. Any activities that are likely to violate the relevant anti-

discrimination law and/or Institute policy or incitement to hatred including but not limited to discrimination on the grounds of race, ethnicity, gender, sexual orientation, disability and religious or political beliefs.

b. Activities prohibited by ICR policy

i. Any activities for personal commercial gain not disclosed and/or authorised by the Institute in writing in accordance with the relevant Institute policy.

ii. Unauthorised orders for goods or services or statements of intent on behalf of the ICR.

iii. Unsolicited commercial or advertising material.

iv. Creation or distribution of materials contrary to medical or animal ethics.

v. Unauthorised or illegal duplication or distribution of any material

covered by copyright, including but not limited to software or publications, is prohibited. Staff and students must ensure that

any copying or duplication complies with the relevant licences and

legal requirements.

7. Use of e-mail, instant messaging and similar services

Chain letters must not be circulated using Institute e-mail service. Institute e-mail must not be automatically forwarded to non-Institute e-mail addresses to avoid compromise of data protection and confidentiality requirements apart from manual forwarding of non-confidential e-mail which would not jeopardise our compliance with the relevant legal or business requirements.

8. Installation and modification of software

Software installed on Institute IT systems (including personal computers) must not be modified without authorisation from a line manager or the IT Department. Software must not be installed on Institute IT

systems (including personal computers) without authorisation from a line manager or the IT Department. Such installations must be in accordance with the ICR's software licensing policy.

9. IT management software

IT management software installed on Institute systems, including but not limited to anti-virus and asset management software, must not be disabled, modified or tampered with.

10. Attachment of devices to Institute systems or network

Attachment of any non-standard equipment must be notified to the IT Department and shall be subject to a risk assessment carried out by the IT Security Manager. In particular, modems, wireless and other networking equipment shall not be connected to the network other than by the IT Department.

11. Unauthorised access

Unauthorised access or attempts to obtain unauthorised access to any Institute systems or data are forbidden.

12. Web presence

Any web presence, including conventional web publishing, micro-sites, social networking presence and related or similar services, relating to the work of the Institute and/or arising from activities funded wholly or in part, directly or indirectly by the Institute must be appropriately branded as ICR and must include standard links to the ICR web site. Branding must also include that of ICR's partners in any work or collaboration, in accordance with any relevant agreements or contracts.

Web publishing will normally be via the ICR web site content management system. Use of any other means of web publishing shall require a valid scientific or business rationale which must be approved by the Divisional or Department Head and must be registered with the ICR Webmaster.

13. Enforcement

Violation of this policy may lead to disciplinary proceedings up to and including dismissal and/or legal action in accordance with the law.

14. Policy Compliance Monitoring

All divisions should ensure that they are able to demonstrate compliance to the principles of

this policy by implementing appropriate procedures, processes and frameworks.

Minimum Compliance Monitoring Expectations:

- As part of the IT induction process, new staff members will be made aware of this policy.
- IT will ensure this policy is updated as required following Internal, Legal & Technological changes.

- IT will review user accounts on a regular basis and ensure that all unnecessary or default user accounts are deleted or disabled
- Where violation of this policy occur, Team leaders are responsible for taking any action that may be required in line with ICR's discip linary procedures.
- Incident reports will be prepared for the Information Governance Committee meeting to ensure a robust governance arrangement.