THE INSTITUTE OF CANCER RESEARCH: ROYAL CANCER HOSPITAL

POLICY

Information Technology Acceptable Use Policy

Committee Approval: Corporate Management Group	Author and Position: IT Security Manager	
Approval Date: 1 July 2011	Department: IT	
Minute Reference: Chair's Action June 2011		
Equality Impact Assessment date: 6 July 2011		
File Name: IT Acceptable Use Policy		Uncontrolled if printed
Review date: 1 July 2011	Reviewed by: IT Director	

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. 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. 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.

5. Explicitly forbidden use

The following activities or uses of Institute IT facilities and services are forbidden. They should not be investigated but should be promptly reported to the HR Director.

5.1. Illegal activities

- Any activities that are illegal under UK law, including but not limited to activities related to terrorism, child pornography, or incitement to violence. 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.
- Creation or distribution of libellous or defamatory messages or statements concerning any individual.
- Creation, access to or distribution of obscene, indecent, bullying, harassing or grossly offensive material.
- 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.
- 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.

5.2. Activities prohibited by ICR policy

- Any activities for personal commercial gain not disclosed and/or authorised by the Institute in writing in accordance with the relevant Institute policy.
- Unauthorised orders for goods or services or statements of intent on behalf of the ICR.
- Unsolicited commercial or advertising material.
- Creation or distribution of materials contrary to medical or animal ethics.
- 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.

6. 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.

7. 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.

8. 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.

9. 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.

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

11. Monitoring and reporting
The Institute reserves the right to monitor IT use in accordance with the relevant law and Institute policy.

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 and those of its partners wherever possible.

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.