Code of Practice for users of the University computing facilities

Contents

1. The Context

Any reference in the following paragraphs to computing services or facilities applies, where appropriate, to those which are available on systems run by IT Services, or sited in Schools or Departments but connected to the University network. To be permitted to use University computing facilities, users are deemed to have read and be bound by this Code of Practice, the University Information Security Policy and the University regulations.

Users need to be aware that their communications may be monitored by IT staff for the business purposes of the University as permitted by Malaysian and UK legislations. The legislations allow the interception of network traffic without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the efficient operation of University communications systems. Users should be aware that their communications could be released to requestors if deemed in the public interest under the UK's Freedom of Information Act (2000).

In cases where there is suspicion of criminal activity or misconduct, further investigation by authorised staff may result in the examination or seizure of any University owned computer equipment or media related to the suspected offence. Examination may include the opening and reading of email, files or other data stores deemed relevant to the investigation. The University may disclose information to the Police or other authorities, as allowed by legislation, in the case of suspected criminal activity.

Access to a user's email, files or data stores related to the University's activities may also be granted to a line manager or authorised alternate if the user is unavailable for their normal duties for a period and the materials are necessary for the efficient operation of the University.

2. Rules for the use of the University computing facilities:

a. access to University computing facilities is normally granted by the issue of an individual username and initial password. The individual concerned is solely responsible for work undertaken from any username issued. Users must only use their own username when accessing the University network. Users are responsible for the security of their passwords. Passwords should never be divulged to anyone and should be regularly changed, whilst ensuring that strong passwords are chosen. Users should be particularly wary of phishing attacks that appear to be official requests for your University username and password, or other personal data, as these may be used for identity theft

b. access to University computing facilities is given and allocations of resources are made for the purposes of the University, as approved by the Department/School, and for the operations and management of the University

c. users must not damage University computer equipment or interfere with systems or any other user software housed on the University computer systems, e.g. by introducing viruses

d. users must not use or attempt to use any network from The University for unauthorised purposes. In particular, the JANET network is subject to the JANET Acceptable Use Policy

e. users must not use or attempt to use any networked service accessed from the University for unauthorised purposes. Use of licensed services must comply with the license conditions. In particular, use of software/datasets licensed through CHEST must comply with the eduserv agreements and the associated User Acknowledgement of Third Party Rights Form

f. all software used on University IT equipment must be appropriately licensed, and proof of such licences must be made available on request

g. information issued by IT Services in official notices, circulars and instructions, and verbal advice given to users is not confidential except where it is stated to be so. However, users are warned to follow strictly any instructions issued regarding the use of proprietary software and any other confidential information. It is strongly emphasised that no such confidential information may be copied, modified or disseminated without the consent of the Head of IT Services or the Head of Department/School, as appropriate

h. users must not access, transmit, store, print, promote or display material where to do so constitutes a criminal offence or a civil wrong. Examples of criminal offences include the possession without a legitimate reason of an indecent photograph of a child; the possession without reasonable excuse of information of a kind likely to be useful to a person committing or preparing an act of terrorism. Examples of civil wrongs include defamation, breach of confidence and the misuse of private information.

i. users should ensure that any information related to University activities and stored locally on their desktop or laptop is backed up on a regular basis. This is to ensure that no vital data is lost. Users are advised to store important data/documents on their cloud drive or on a shared drive
j. users should adhere to the rules and regulations surrounding the use of social networking sites (for example not posting material in such a way as to bully or harass, or to bring the University into disrepute) – see the Social Media Policy for Staff and Social Media Policy for Students
k. users must not use any third party materials (including images, databases, text, sounds, logos, trade marks) in any documents (including emails and web pages) in breach of that person's intellectual property rights. As a general rule, users must not copy any third party material unless the permission of the owner has been obtained
l. users must not send unsolicited bulk emails (spam)
m. all computing use must comply with relevant legislation, in particular with the UK's Data Protection Act (1998), Human Rights Act (1998), Copyright, Designs and Patents Act (1988), Computer Misuse Act (1990), Privacy and Electronic Communications (EC Directive) Regulations (2003), Freedom of Information Act (2000) , Counter-Terrorism and Security Act 2015 and the Malaysian's Copyright Act 1987 (Act 322), Computer Crimes Act 1997 (Act 563), Communications and Multimedia Act 1998 (Act 588), and all other relevant legislation, in both UK and Malaysia
n. users must comply with the borrower agreement for the loan of University laptops and tablets
o. projects sponsored by outside bodies should not make use of University IT facilities without prior consent of the Head of IT Services (or nominee)

3. Infringement of the Code of Practice

Users of the University computing facilities who are found to be in breach of the above rules may be liable to disciplinary action under the relevant provisions for staff and students. Disciplinary action may take the form of, but is not limited to, withdrawal of access to computing facilities, the giving of an oral warning or written warning, the imposition of a fine, or the suspension or expulsion of the relevant staff or student.