The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

Borrower agreement for the Learning@the Core Plasma Smartboard or LCD TV Devices loan service

1. I accept that each time I borrow the Plasma Smartboard or LCD TV Devices package, I will take custody of the equipment indicated below, in good condition

* Wireless mouse

* Keyboard

* USB adaptor (Toggle)

* Remote control

* Smart Pen (only valid for Plasma Smartboard Devices package)

* Airpad (only valid for LCD TV Devices package)

You are responsible for the safe return of all parts of the package after each loan period.
Upon return, the package will be checked by Student Adviser for loss and/or damage.

2. I agree to use the equipment safely. I agree to protect the equipment from theft and/or damage.

3. I understand that the University will investigate the damage to or loss of the equipment. I will cooperate in the investigation.

4. I agree to notify Student Adviser immediately if the equipment is damaged, lost or malfunction.

5. I agree to return the Plasma Smartboard and LCD TV Devices before the due time/date or upon request by Student Adviser.

6. I agree to pay fines for late return (RM10.00) per hour or part of an hour, non return (RM600) or damage (up to a maximum of RM250.00) may be incurred

7. I understand that Plasma Smartboard and LCD TV Devices loan is not transferable.

Date: ……………………………… Name: ……………………………………………………………..

H/Phone: …………………………. Library number: ……………………………..Signature: ……………………

Code of Practice for Users of the University Computing Facilities

1. In the following paragraphs any reference to computing services or facilities applies, where appropriate, to those which are available on systems run by Information 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 for the business purposes of the University by IT staff as permitted by Malaysia 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 Freedom of Information Act (2000).

In cases where there is suspicion of criminal activity or gross 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 opening and reading 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 the 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 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 request 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 purpose of the University, as approved by the departmental/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 subjected to the JANET Acceptable Use Policy and the campus Internet link is subject to the local ISP terms and conditions.
e. Users must not use or attempt to use any networked service (e.g. BIDS, Edina etc.) 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 CHEST Code of Conduct and its associated Copyright Acknowledgement.
f. All software used on University IT equipment must be appropriately licensed, and proof of such licenses must be made available on request.
g. Information issued by Information 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 Information Services or the Head of Department/School, as appropriate.
h. Users must not access, transmit, store, print, promote or display offensive, obscene or indecent material (for example pornography; material that is discriminatory on the grounds of sex, race disability or religion; material likely to incite hatred, terrorism or violence), defamatory materials or materials likely to cause harassment, alarm or distress.
i. 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, to bring the University into disrepute - see also the Statement from the Registrar on this issue).
j. Users must not use any 3rd party materials (including images, databases, text, sounds, logos, trade marks) on any documents (including emails and web pages) either in breach of the person's intellectual property rights and/or without consent of the owner.
k. Users must not send unsolicited bulk emails (spam).
l. All computing use must comply with the relevant legislation, in particular with the Data Protection Act (1998), the Human Rights Act (1998), the Copyright, Designs and Patents Act (1988), the Computer Misuse Act (1990), the Privacy and Electronic Communications (EC Directive) Regulations (2003), the Freedom of Information Act (2000), the Copyright Act 1987(Act 322), the Computer Crimes Act 1997 (Act 563), and all other relevant legislation, both in Malaysia and UK.
m. Users must comply with the borrower agreement for the loan of University laptops.
n. Projects sponsored by outside bodies should not make use of University IT facilities without prior consent of the Head of Information Services (or nominee).

3. Users of the University computing facilities who are found to be in breach of the above rules are 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.