ESCP Business School Conditions of Use of Computing Facilities

The following conditions of use are applicable to all usage of computers and networks at ESCP Business School London including office based and stand-alone systems.

It should be noted that these conditions form part of the School's conditions of employment and student regulations; breach of these regulations, particularly in relation to Data Protection and obscenity, may lead to disciplinary action. The more serious breaches may be considered under gross misconduct.

All users should be aware that by registering with us you have agreed to abide by these Computing Services "Conditions of Use". Remember that password security is key to ensuring that your account is not misused. Take care of your password - do not share it or email it to anyone and avoid writing it down.

Legality

All users of ESCP systems are expected to comply with relevant legislation. This includes the following Acts of Parliament:

Computer Misuse Act 1990;

The full text of this Act is available from the HMSO web site at http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm.

Copyright, Design & Patents Act 1988;

The full text of which may be found on the HMSO website at http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

Criminal Justice Act 1994;

The full text of this Act is available on the HMSO web site at http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm.

Data Protection Act 1998;

The full text of this Act is available on the HMSO web site at http://www.legislation.gov.uk/ukpga/1998/29/contents

Freedom of Information Act (2000);

The full text of this Act is available on the HMSO web site at http://www.legislation.gov.uk/ukpga/2000/36/contents

Regulation of Investigatory Powers Act (2000);

The University is required under the Regulation of Investigatory Powers Act (2000) to bring the following notice to the attention of all its users:

As required by UK legislation, Computing Services draws to the attention of all users of the School's data network the fact that their communications may be intercepted as permitted by legislation. The legislation allows the School to intercept without consent, for purposes such as recording evidence of transactions, ensuring regulatory compliance, and detecting crime or unauthorised use. The School does not need to gain consent before intercepting for these purposes, although staff and students of the School should be advised that interceptions may take place.

Telecommunications Act 1984;

The full text of this Act is available on the HMSO web site at http://www.legislation.gov.uk/ukpga/1984/12/contents and laws on obscenity, indecency, defamation and financial services. In some cases legislation in other countries may also apply.

Resource Usage

Facilities provided by the School are intended to be used in furtherance of the aims and objectives of the School. A reasonable amount of personal use is permissible but:

- priority - especially at peak periods - must be given for the intended use;
- networks - through which all our internet traffic passes - may have their own Acceptable Use Policies which must be complied with;
- licence conditions on some software or data may limit the nature of usage;
- work of a commercial nature, or for reward, and including web sites for external organisations requires prior written permission;
- the provision of any service to non-members of the School also requires such permission;
- a number of external resources are accessible by users of the School's computing systems and networks. There are specific conditions of use which govern the use of these resources. Access is given to users under the following conditions:
- users will ensure that all the requirements of the Agreements under which the services are held by ESCP will be maintained. Details of the Agreements are available from the Business Librarian or the IT Manager.
- users will ensure that any copyright statement is maintained on any copies of the information used.
- users will ensure the security and confidentiality of the database made available to them and will not make any further copies from it except and insofar as this may be permitted within the terms of the Licensing Agreement.
- users will use the information derived from the databases only for purposes defined in the Licence.
- please note that ESCP reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of violation of its Licensing Agreement.

Interference with Others, Obstruction

Behaviour that has the potential to disrupt the work of others, or can reasonably be considered offensive by them, will not be tolerated. This can include:

- the display of offensive material
- invasion of privacy
- unauthorised access to their files
- and harassing emails.

Potential for harm

Certain activities that are not, of themselves, necessarily illegal or damaging are restricted because they may pose a risk of damage, of expensive consequences, or of harming the reputation of the School. Specific rules of this nature include:

- The storage or publication of information (including on web sites) intended to breach copyright or security is forbidden. Some copyright material may be used for teaching - see the Business librarian for guidelines;

- keep mobile phones switched off at all times in the workstation rooms;
- the unauthorised use of network monitoring software is forbidden;
- care should be taken not to imply that a personal statement describes School policy;
- Avoid defamatory statements, especially in "public" messages (web pages, newsgroups, bulletin boards, and mailing lists).

Investigation and Enforcement

Certain activities on the network and centrally provided systems are routinely logged and/or automatically monitored. These include:

- Usage of workstations
- Access to web pages
- Access to software
- Volume of data transfers
- Quantity of email.

In the majority of cases, the primary purpose of such logging is for fault investigation and capacity planning, anomalies may prompt investigation of possible breaches of the Conditions of Use and the information is available when evidence of possible misuse is needed.

You are advised that Computing Services will regularly scan both the School web cache for obscene material as part of the Policy on Obscene material and the network to detect any vulnerable shared directories.

- The School does not seek to lay down codes of moral behaviour in this area; however, it is bound by the law, by the conditions of use of the network, and may be subject to sanctions if it does not take seriously the guidance.
- Using the School's network to send or receive obscene material is a breach by the user of conditions of use and additionally may render the School liable to criminal proceedings as a distributor of such material. The School must therefore institute a pro-active policy to deter such misuse of facilities.
- It is important to distinguish different kinds of offence. Leaving child pornography aside, the act of viewing obscene material on the internet is not a criminal offence, though it contravenes conditions of use. Any disciplinary consequences should therefore be proportionate and should follow informal warning, initially from the UK Director. By contrast, the distribution of obscene material (including the circulation of it to another user) is capable of being a criminal offence and should be dealt with under the disciplinary procedures, which provide for discretion in the matter of reporting it to the Police.
- Offences involving child pornography should be reported to the Police in all cases.

When required further information may be collected - this is normally only performed in response to an investigation prompted by a specific complaint. Such a complaint may have been from the managers of remote sites and networks, from users, from the police, or as a result of an investigation prompted by an anomaly in routine monitoring. In these cases, where not forbidden by law, the School reserves the right to:

- inspect network traffic between a user's machine and any other address(es)
- inspect - possibly via an automated search - the content of files held on any system managed by Computing Services and on any system - even privately owned - that is, or has recently been, connected to the campus network.
- inspect email, both incoming and outgoing. Further restrictions may be employed in the event of warnings about harmful software (eg viruses and worms) or security problems being received.

- cut off access (either by disabling logins or by disconnecting from the network) where it is considered advisable to prevent further misuse.

Email cannot be safely considered to be completely private and there should be no expectation of privacy. You should abide by the School's Email Acceptable Use Policy.

This Email Acceptable Use Policy applies to all School staff (including temporary staff), visitors, contractors, students and researchers of this School and to those using the School's IT resources. This policy should be considered part of the Conditions of Use for Computers and Networks at School.

General Principles

- Use of email by the School employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the School and its business units. Email is to be used in a manner that is consistent with the School's standards of business conduct and as part of the normal execution of an employee's job responsibility.
- School email accounts are to be used for School business. Limited personal use is considered acceptable.
- The School will directly access staff email accounts in the pursuit of an appropriately authorised legal or disciplinary investigation.
- Use of email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.
- The distribution of any information through the School's network is subject to the scrutiny of the School. The School reserves the right to determine the suitability of this information.
- The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. For example the Police can have a right of access to recorded data in pursuit of a crime.
- Email messages are treated as potential corporate messages of the organisation.
- The School reserves the right to redirect the email of staff that have left for legitimate business purposes. Users are responsible for ensuring personal emails are stopped.

Unacceptable Use or behaviour:

It is unacceptable to;

- Solicit emails that are unrelated to business activities or for personal gain.
- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Represent personal opinions as those of the School.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the School, or the School itself.
- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, databases and the information contained therein, computer network access codes and business relationships.
- Waste time on non-School business.

Users should:

- Keep emails brief and use meaningful subject lines.
- Re-read messages before sending to check for clarity and to make sure that they contain nothing which will embarrass the organization or make it liable.
- Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email.
- Use file compression techniques for large documents or send then using an alternative method.
- Archive effectively - use folders and delete any messages you no longer need.
- Don't overuse the "URGENT" flag as it will lose its value.
- Never reply to spam.
- Avoid using email for sensitive or emotional messages or offensive content.
- Take care in drafting emails, taking into account any form of discrimination, harassment, School representation, and defamation of Data Protection issues.
- Staff Emails are a form of corporate communication and therefore should be drafted with the same care as letters.
- Users should be careful when replying to emails previously sent to a group.
- Ensure your terminal is locked or logged out when you leave your desk, a malicious user could send messages in your name.
- Avoid 'Mail Storms' - long discussions sent to a distribution list - consider verbal communication or use a bulletin board.

Monitoring

The School accepts that the use of email is an extremely valuable business, research and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the School's public profile. As a result;

- The School maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation.
- The specific content of any transactions will not be monitored unless there is a suspicion of improper use.
- We are obliged to monitor to fulfil our responsibilities with regard to UK law.

The IT department may also examine any School owned computer for unlicensed software and test the security of any computer connected to the School network.

Except where it provides evidence of a breach of these conditions, of serious criminal activity, or of significant costs to the School, information acquired during any monitoring will be kept strictly confidential to those directly involved in the investigation. In the case of serious criminal activity the information will be made available to the police.

Serious breaches of these conditions will be handled by the School Disciplinary Procedures and may result in dismissal. The School also retains the right to report any illegal violations to the appropriate authorities.