ISC10D0498

Conditions of Computer Use

Policy and guidelines governing use of all University IT and network facilities

Approved by the Information Strategy and Service Committee 16th June 2011

Revisions for 2011/2012 academic year

- Table of contents – 'U' of university capitalised in title for 3.1

- Changed "ICT Policy Manger" to " Assistant Director Strategy, Policy and Compliance" throughout to reflect new structure for 2011/12 academic year.

- 2a - Text in capitals changed to emphasise that user should not respond to any request to disclose password including uea OR Information Services.

- 2j - Text changed to emphasise responsibility of owner for activity on their system. Students have tried to 'wriggle' out of their responsibility in some computer misuse incidents.

- 3.10e - Added in addition to above in order to emphasise responsibility of registered owner for inappropriate activity arising from a computer. Also added footnote to clarify situation re. shared systems where IT support are registered owner.

- 3.11h - Added text to emphasise General Student Regulation that students should be in a position to respond to University communications within 48hrs. This has been a problem when dealing with some incidents. Also inserted in Summary Conditions as 2l.

- 3.11f - Added text "Users should never send their UEA password in an e-mail. Any e-mails which asks for your password is a hoax" to aid the user education campaign regarding not responding to phishing emails. Note, importance of not disclosing passwords is also dealt with in several other places including the 'Summary Conditions'.

- 3.14i – Revised to reflect disposal arrangement as part of contract for Managed Service for PC Procurement.

- Section 8 – Footnote added sating when last major review was done. Some changes to reflect new support structures, "Directors of Faculty Administration" removed.

Information Services
I.T. & computing

Contents

Information Services
I.T. & computing

1. Purpose and Scope

These Conditions of Computer Use are a formal statement of what is acceptable and unacceptable when using the University's IT facilities and network. They aim to encourage responsible behaviour and good practice, thus assisting the University in maintaining a secure, safe and robust IT environment. The conditions detailed here apply to all using the University's IT facilities whether a member of staff, a student, or a person from outside the University who has been authorised to use facilities.

All those using the University's IT facilities and network should be aware of these conditions and abide by them. Contravention of these conditions could lead to disciplinary action and loss of access to IT facilities. If you are unsure about any aspect of these Conditions of Use or your use of UEA's IT facilities, it is your responsibility to seek clarification by contacting the University's IT Helpdesk (see section 7 for contact details).

Information Services will make all users aware of these Conditions of Computer Use when they are issued an IT account. Reminders will also be communicated on a regular basis. It is also the responsibility of each Faculty or Division and their constituent Schools/Departments to ensure that this document is brought to the attention of users within their domain during induction processes for new staff and students and at other times when appropriate.

2. Summary Conditions

a) Your UEA password is confidential and you must never disclose it to others, or let anyone else access services and systems using your password. Disclosing your password to others contravenes the Conditions of Computer Use and could lead to disciplinary action and loss of access to IT facilities. YOU SHOULD NOT RESPOND TO ANY REQUEST TO DISCLOSE YOUR PASSWORD INCLUDING THOSE PURPORTING TO COME FROM THE UNIVERSITY OR INFORMATION SERVICES. See 3.4j.

b) Be aware of relevant legislation. In particular, if you work with personal information about individuals, you must be aware of and comply with the Data Protection Act. You should also be aware that University computer communication systems are dependent on the Joint Academic Network (JANET) and all use must comply with JANET's Acceptable Use Policy. See section 3.2

c) Computing facilities are provided for University work purposes. Limited personal use is permitted provided it is not illegal, does not adversely affect other users, does not interfere with work or studies, or in any other way breach the Conditions of Computer Use. See section 3.3.

d) Care must be taken to ensure you do not create, transmit or publish any material that is illegal, offensive, abusive, or liable to bring the University into disrepute. See section 3.4.

Information Services
I.T. & computing

e) Files are private. You must not attempt to access files or computer systems which you are not authorised to access. See 3.4i.

f) Electronic media are subject to copyright. It is illegal to make an electronic copy (e.g. by scanning, downloading, copying from disk etc.) unless you have the appropriate copyright authorisation. See section 3.7.

g) Software is subject to copyright and licensing restrictions. Software provided by the University should only be used by members of the University for University purposes and in accordance with licence conditions of the software. You should not install, copy or distribute it to others unless authorised to do so. See section 3.8.

h) Care must be taken when introducing software/data into the University. Only those authorised to do so should install data or software onto University computer systems (desktop systems, laptops/notebooks and servers) and they should ensure it has been checked for viruses or other malware. Do not transmit files/data to others, without first checking for viruses or other malware. See section 3.9.

i) If you are responsible for supporting others and the systems and services they use, you have an additional responsibility to ensure that those systems and services are secure, and should encourage good practice in those that use them. Ensure computer systems in your care are secure against unauthorised access and malware, have up to date operating system and application software security patches applied and anti-virus/anti-malware software is installed and is up to date. See section 3.14.

j) All personally owned computers connected to the network must be registered following processes described at http://www.uea.ac.uk/is/itregs/equipreg . Where a computer has been registered using an authorised self-registration process (e.g. in student residences) the owner is responsible for security of that system and any activity on it. Should inappropriate activity be detected arising from the computer the registered owner will be held responsible for that activity. The owner should ensure that the system has up to date operating system and application software security patches applied and up to date anti-virus/anti-malware software is installed. See section 3.10.

k) Use of University computer systems and the network is monitored. The University has the right to access files, intercept communications, or monitor usage where there are grounds for suspecting mis-use. In cases where illegal activity is involved copies of relevant information may be handed to the Police at their request. See section 4.

l) Students are reminded that the University's General Regulations for Students require them to be in a position to respond to any notice or communication directed to them within 48 hours of it being made available to them i.e. of it being posted on a notice board, on their University e-mail account or in their pigeonhole

3. Conditions of Use

Information Services
I.T. & computing

3.1 Access to University IT facilities

Use of the University's IT facilities and network is restricted to the following registered users:

(a) Students registered with the University for a programme of study.

(b) Staff holding a contract of employment with the University.

(c) Other individuals who have been sponsored by the relevant Head of School/Department, or their nominated deputy and authorised by Information Services.

Further information on the above and the facilities and services that they are entitled to use, are detailed in the Information Services Directorate (ISD) User Entitlements Policy which is available at http://www.uea.ac.uk/is/user-entitlement-policy.

3.2 Relevant legislation

All users of the University's IT facilities are bound by current relevant legislation and by the JANET (Joint Academic Network) Acceptable Use Policy. Further information is available from http://www.uea.ac.uk/is/itregs/extleg.

3.3 Acceptable use

a) Computing facilities are provided for the pursuit of legitimate University activities:

    i)   Teaching and learning.

    ii) Research.

    iii) Personal educational development.

    iv) Administration and management of University business.

b) Limited use of the University network and IT facilities for personal purposes other than UEA work or study, for instance personal correspondence via e-mail or access to the internet, is permitted. However such use must not interfere with work or studies, must be legal and must be strictly in accordance with the requirements laid down in these Conditions of Computer Use.

3.4 Unacceptable use

All of the following are expressly forbidden when using the University's network and IT facilities:

a) Any illegal purposes. The Police will be informed where there is evidence of illegal activity.

b) Accessing, creating, storing or transmitting (other than for properly supervised and lawful research purposes*) offensive, obscene or indecent data or images, or data from which such material could be derived *Where research is likely to include such material, authorisation should be sought from the Head of School and the relevant research or ethics committee and the

Information Services
I.T. & computing

Information Services Assistant Director Strategy, Policy and Compliance made aware.

c) Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.

d) Creation or transmission of defamatory, discriminatory or libellous material, or material likely to bring the University into disrepute.

e) Transmission of material that infringes the copyright of another person.

f) The unauthorised distribution to third parties of any information in which the University and/or partner organisations such as research funders have intellectual property rights.

g) Unauthorised interception or hacking of communications over the network including but not limited to e-mail and telephone messages.

h) The transmission of unsolicited commercial or advertising material either within the University or externally, unless authorised to do so on behalf of the University.

i) Unauthorised access or attempting to gain unauthorised access to IT facilities or services both within and outside the University.

j) Disclosing your UEA password to others, or letting others use your UEA IT account[1], irrespective of whether they are members of the University.

Users are responsible for the security of their password and should under no circumstances disclose this to others, whether in response to an e-mail, by visiting a web page, in person, or over the telephone; neither should they allow others to use their IT account (including members of UEA or external parties). Failure to comply with this may result in loss of access to facilities and/or disciplinary action. If a user has previously been detected as having disclosed their password to others and after having been duly warned is discovered to have disclosed their password on a subsequent occasion, they will lose access to IT facilities and the matter will be reported to the appropriate University disciplinary authority for further action.

k) Deliberate activities with any of the following characteristics:

   i) Corrupting or destroying others users' data.

   ii) Violating the privacy of others.

   iii) Disrupting the work of others.

   iv) Seeking to bully or harass others.

   v) Causing annoyance to others by inappropriate or inconsiderate use of computing facilities (e.g. internet phones in IT areas).

   vi) Using applications for non-academic purposes which are likely to result in excessive network traffic causing disruption to others.

---

[1] Where an individual is absent from work for a prolonged period and access to their IT account is required in order to progress University business, access to another authorised individual can be granted if authorised by the relevant Head of School or Department.

Information Services
I.T. & computing

vii) Continuing to use an item of software/hardware after Information Services has requested that such use cease.

viii) Misuse of University IT facilities or resources in such a manner that it compromises the security of University systems and the network.

3.5 Data protection and security

The University is required to keep certain personal data about staff and students in order to fulfil its objectives and to meet legal obligations. The law requires that this data must be collected and used in a fair manner, stored securely and not disclosed to any other person unlawfully.

a) No user may use the University's computer systems to hold or process personal data except in accordance with the provisions of the Data Protection Act (DPA) 1998.

b) Staff must not construct or maintain computer files of personal data unless required to do so as part of their work responsibilities and as approved by their manager.

c) Students must not construct or maintain computer files of personal data for use in academic studies or research without the express authority or an appropriate member of staff, normally their supervisor or Head of School.

d) Those in the University who have data in their care, or who are authorised by the University to process personal data, should ensure that they are aware of their obligations under the Data Protection Act and comply with the Data Protection principles. These principles along with more information about the Act and its applicability at UEA can be found at http://www.uea.ac.uk/is/strategies/infregs/dp.

e) Where users have University data in their care, they should also be aware of and comply with the following:

i) The University's General Information Security Policy - see http://www.uea.ac.uk/is/itregs/ictpolicies/generalinformationsecuritypolicy.

ii) All University data should be assessed on its strategic value and level of confidentiality and stored and handled in accordance with policies and controls detailed in the Information Classification and Data Policies. These are linked to from the following web page:

https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman

f) Data relating to University research, teaching and administration should only be stored on University provided and approved systems.

g) Managers of staff with data responsibilities must ensure that their staff follow University security policies and advice, and in general adopt good practices in this regard.

3.6 Freedom of information

The Freedom of Information Act (FOIA) 2000 gives everyone both in and outside the University a right of access to any recorded information held by the University. In order to meet its obligations under the Act, the University must respond in an appropriate and professional manner to all FOIA requests. University staff, particularly those with responsibilities for recorded data, should be therefore be aware of and follow the guidelines at http://www.uea.ac.uk/is/foi/guidance-for-staff .

3.7 Copyright

a) Copyright material may only be copied if the copyright owner has granted permission, either directly or through a licensing scheme.'Copying' includes scanning, recording and downloading, and covers print, digital and web based material.

b) Copyright material should not be networked or otherwise transmitted to multiple recipients without first getting the rights owner's permission, or ensuring that such action is covered by an appropriate licence.

For more guidance on copyright see the web page at http://www.uea.ac.uk/is/strategies/infregs/copyright.

3.8 Software

a) Software is subject to copyright and licensing restrictions and persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.

b) Software provided by the University should only be used by members of the University for University purposes and in accordance with licence conditions of the software. You should not copy or distribute it to others unless authorised to do so.

c) In general, all users are expected to honour any agreements or contracts made by the University concerning any computer software or data that they use and to abide by the general principles as detailed in the Software Copyright Acknowledgement document which is available at http://www.uea.ac.uk/is/itregs/softwarecopyright.

d) Software Licence Agreements vary. The principal user of a single user system or the manager of a multi-user or networked system is responsible for the software loaded on that system and ensuring that it is used in accordance with the licence agreement.

e) Only approved software that is being used for University work purposes may be installed on to University owned computers. Approval must be sought prior to any installation from the relevant School/Department's member of IT support staff responsible for the equipment. In most cases IT support staff will carry out the installation.

Information Services
I.T. & computing

f) Software provided by the University should not be deleted, disabled or altered, other than by authorised personnel.

g) Users must co-operate with persons employed by the University to carry out software and data audits, and where required follow software registration procedures.

h) Schools /Departments must keep an up-to-date inventory of all software installed on their computers and ensure that no software is installed for which the University does not have a current licence.

i) Schools/Departments must also ensure that any University licensed software is returned by leaving members of staff or students and any copies are removed from computers within their care, prior to leaving the University.

3.9 Computer security

a) All access to computers and the network should be authenticated by use of a UEA Username and UEA Password. Strong passwords should be used following advice published at http://www.uea.ac.uk/password and complying with the University's password policies as defined in the Security Manual at https://intranet.uea.ac.uk/is/itregs/ictpolicies/secman.

b) All IT equipment under the University's care should be maintained in a secure manner in accordance with the General Information Security Policy and Security Manual. IT support personnel have a particular responsibility in this regard.

c) All computers connected to the University's network should have up to date operating system and application software security patches applied and anti-virus software installed, irrespective of whether they are owned by the University, or personally owned. For university owned systems these should be installed and configured according to Information Service's recommendations with auto updating enabled and following guidelines and policies defined in the General Information Security Policy and Security Manual.

d) Only those authorised to do so should install data or software onto University computer systems (desktop systems and servers) and they should ensure it has been checked for viruses or other malware. Users should not transmit files/data to others, without first checking for viruses or other malware.

e) Information Services reserves the right to disconnect any computer from the network that is discovered to be infected with malware (e.g. viruses, trojans), or does not have adequate virus-checking software installed.

3.10 Connecting equipment to the network

a) All client machines connected to the University's network must be individually registered and authorised following University approved policies and processes detailed at http://www.uea.ac.uk/is/itregs/equipreg.

b) No equipment (whether University or user owned) should be used to extend or provide additional connections, for example via wireless transmitters or routers, unless approved for this purpose by Information Services.

c) User owned computers which have been authorised and registered using self registration processes detailed at http://www.uea.ac.uk/is/itregs/equipreg, must also comply with the additional Self-registered Equipment Terms and Conditions detailed at http://www.uea.ac.uk/is/itregs/selfregtc.

d) The University reserves the right to prohibit the use of equipment which is likely to cause interference on frequency ranges used by the University's wireless network.

e) The registered owner of a computer will be held responsible for any inappropriate activity arising from that computer[2]. In the case of personally owned systems the owner is responsible for ensuring that the system has up to date operating system and application software security patches applied, and up to date anti-virus/anti-malware software is installed.

3.11 Electronic mail

a) Only Information Service's approved and provided systems should be used by staff for e-mail communications concerning University matters. For a list of approved systems see https://intranet.uea.ac.uk/is/itregs/ictpolicies/staffemail.

b) E-mail systems provide a written record and care should be taken when composing and sending messages to ensure that the intended meaning is conveyed and the message is delivered to the intended recipients. Good practice guidelines on using e-mail are published at https://intranet.uea.ac.uk/is/itregs/userguide/emailguide.

c) The Data Protection and Freedom of Information Acts also apply to e-mails containing personal data. Such e-mails must be stored and processed in accordance with the Data Protection Act and may have to be released in response to Freedom of Information Act requests. For more information on these acts see sections 3.5 and 3.6.

d) E-mails which infringe the copyright of another person should not be passed on.

e) Anything sent electronically, including e-mail, is susceptible to interception. Users should whenever possible avoid sending highly confidential or sensitive information by e-mail. If it is essential to do so, the information should be contained within a password protected file attached to the message. The password should conform to the University's password policies and guidelines detailed at http://www.uea.ac.uk/password and should be communicated to the intended recipient by other means.

f) Users should never send their UEA password in an e-mail. Any e-mail which asks for your password is a hoax.

---

[2] For University owned/managed desktop computers where more than one user shares the system and the computer is registered with an IT support manager or deputy, the system must be set up in such a manner any user responsible for inappropriate activity can be identified.

Information Services
I.T. & computing

g) Before sending an e-mail users should assess whether the message is representing University views and whether the information is confidential, and make this clear within the message. A liability disclaimer and confidentiality statement should be added to the message if appropriate; links to recommended text for these are provided at http://www.uea.ac.uk/is/email.

h) Only a user's UEA assigned e-mail address will be used to send e-mail messages from the University to the user. Users wishing to read their e-mails from the University using an external service provider's e-mail system are responsible for changing the settings on their UEA e-mail account so that messages are automatically forwarded to the external service provider's system. Staff should also be aware of 3.11a above. Students are reminded that the University's General Regulations for Students require them to be in a position to respond to any notice or communication directed to them within 48 hours of it being made available to them i.e. of it being posted on a notice board, on their University e-mail account or in their pigeonhole.

i) Users should note that their use of the University e-mail system is not private and that whilst continuing to maintain the privacy of personal mail, the University reserves the right to inspect and disclose the contents of e-mails under special circumstances as declared in section 4 'Monitoring and Privacy'.

3.12 Internet publishing

a) Users should be aware that sending electronic mail to any extended group including but not limited to social networking sites and blogs, or even to a list of recipients, is considered to constitute its publication. Likewise, placing information onto a computing system in such a way as to make it accessible via the World Wide Web is considered to constitute its publication.

b) No item should be published using the University's facilities that could be considered to be defamatory, discreditable or injurious to the University's reputation, that in any way contravenes current legislation, or that could result in any violation of the JANET Acceptable Use Policy. The University reserves the right to remove any such material and to remove access rights in order to prevent further publishing of such material.

c) The University may allow users to publish information over which it does not exercise any specific editorial control. However, unless the user has been duly authorised to act officially on behalf of the University, it disclaims all responsibility for such publications and asserts that the user will be held responsible for any infringements of law or applicable regulation, and for any consequent claims.

d) Where the University has not duly authorised the user to act officially on its behalf, the user must make it clear that the views they express are their own and do not reflect those of the University or their individual School/Department. An explicit disclaimer should be included unless it is clear from the context that the author is representing the University or their School/Department. A standard disclaimer for addition to e-mails sent to external parties is available from https://intranet.uea.ac.uk/is/itregs/userguide/emaildisclaim.

Information Services
I.T. & computing

e) Users should ensure that any information that is posted on a University website is accurate and reviewed regularly (at least on an annual basis).

3.13 Use of services provided by others

(a) If a service provided from outside the University is accessed by means of University facilities then users must also abide by that provider's conditions of use, code of conduct, policies or rules relating to the use of that service.

(b) In order that the University may comply with its licences for access to electronic resources (including databases and electronic journals), users shall ensure the security and confidentiality of the electronic resources made available to them. In addition, users shall ensure that any information derived from these resources is used only for the purpose defined in the licences. Copies of these licences, which include details of copyright restrictions, are available for inspection on application to the Main Library.

(c) If a user connects to external services using the University network and internet connection in order to carry out personal transactions such as purchase of goods or banking transactions, the University accepts no liability for those transactions, or for the security of any personal data transmitted.

3.14 Staff providing IT and service support

It is recognised that in the course of their duties University staff providing IT support, or support for University provided services, may have access to confidential information stored on computer systems. IT support staff also have special responsibilities in regard to ensuring security of computer systems within their care. The conditions detailed below apply to all staff that provide IT support, or support for IT based services and are in addition to those conditions listed elsewhere in this document:

(a) Support staff will only actively seek information on a computer that is relevant to the work being carried out. Specifically they will not open files or e-mails on a user's computer, or in a user's computer account, unless necessary to solve the problem being investigated.

(b) Support staff will maintain strictest confidence and will not divulge confidential information stored on a computer or in a computer account to others unless they suspect that illegal activity or activity that contravenes the Conditions of Computer Use has occurred. Note, monitoring of access to UEA centrally provided services such as e-mail and the network is undertaken by IT support staff in order to maintain service efficiency and prevent problems. Such monitoring will not involve access to a user's computer account/resources unless authorised by the Assistant Director Strategy, Policy and Compliance or a member of the ISD Management Team who will be responsible for overseeing such activity.

(c) When a computer system is temporarily removed from a user's office in order to carry out work on it, IT support staff will ensure that the equipment is housed in a secure environment so as to prevent unauthorised access or theft.

(d) Users' passwords will not be re-set or divulged to others, except:

Page 12

Doc. Ref. CoCU111/12   Date. 06/06/2011
Contact. S.Mosley@uea.ac.uk   Author. Steve Mosley

Information Services
I.T. & computing

    i.   Where a re-set is required for security reasons.

    ii.   Where the user is unable to access their account because they have forgotten their password. In this case their password will be re-set and communicated to them

    iii.   Where a member of staff is absent and the Head of School or Department, or their deputy, requests access to the user's account in order to carry out the business of that Department. In this case the password will be reset and this conveyed to the appropriate person requiring access.

(e) Support staff should not expect or request that a user should disclose their password.

(f) 'Administrator' passwords should not be divulged to anyone except authorised staff engaged in support work where that work cannot be done without such access. Additionally, administrator privileges should not be assigned to any individual's IT account unless they are authorised to undertake work which requires this.   An auditable log should be maintained of those issued with Administrative passwords and the password reset whenever a person is taken off this list or leaves the University.

(g) Permissions and privileges giving access to a user's computer, IT account, e-mail account, or stored files and data should not be altered unless for good reason and with the knowledge and agreement of the user, except where requested to do so for investigative purposes and with approval of the appropriate persons (see section 4 'Monitoring and Privacy').

(h) IT support staff will not make a connection to a computer over the network without the prior agreement of the system owner or, in their absence and for operational reasons, the Head of the Department concerned or their deputy. This includes mapping network drives with Administrator passwords and connection to PCs using remote desktop tools. If such a connection is required for investigative purposes, this must be authorised by the Assistant Director Strategy, Policy and Compliance or a member of the ISD Management Team.

(i) IT support staff will only dispose of unwanted computers or data storage devices using the disposal service included within the University's Managed Service for PC Procurement contract. This service will guarantee that all data is deleted in such a manner that it cannot be recovered. Details about the service will be published on the Purchasing Office web pages (https://www.uea.ac.uk/fin/purchasing).

(j) If a computer or data storage device is transferred within UEA for use by another user or department, any data stored on the system should be erased in accordance with HMG Infosec Standard 5 Enhanced[3] criteria to ensure any previous owner's information cannot be recovered.

(k) IT support staff are responsible for the good security of systems within their care and for encouraging where possible the good security practice of individuals using

---

[3] A standard for erasure of data determined by the Computer-Electronics Security Group (CESG) which is part of the UK Government Communications Headquarters (GCHQ)

Information Services
I.T. & computing

those systems. Policies and controls as detailed in the [General Information Security Policy and in the Security Manual](#) should be adhered to. If requested by a user to undertake work which they feel would compromise security, they should advise against this and if appropriate discuss with their line manager and/or the user's line manager.

4. Monitoring and Privacy

a) The University reserves the right to monitor use of the University network, associated telecommunication systems and the Internet by users and, if necessary, to withdraw access if it is felt that it is being used excessively for purposes unconnected with and/or to the detriment of work/studies.

b) Routine monitoring takes place for maintenance, fault-finding purposes and enforcement of these Conditions of Computer Use, which may reveal unencrypted data and sites visited by users to operational staff. More detailed monitoring may also be undertaken if there are reasonable grounds to believe that a user has committed a criminal offence or is otherwise in breach of the Conditions of Computer Use.

c) Users should note that University facilities are provided primarily for University work, study and business purposes and that whilst continuing to maintain the privacy of personal information, the University reserves the right to inspect and disclose information stored on University IT systems, including the content of e-mails, web pages and files under the following circumstances:

   i) To locate substantive information that is required for University, School or Department business.

   ii) To set up an automatic reply or forward mail if members of staff are unexpectedly absent or have gone on leave without making forwarding arrangements.

   iii) In the course of an investigation triggered by indications or allegations of misconduct, misuse, or illegal use.

   iv) To respond to legal processes, or to fulfil the University's obligations to third parties or in other exceptional circumstances, e.g. medical emergency.

5. Breaches of these Conditions of Use

(a) If there are reasonable grounds for suspecting that a user is engaging in activities which are in breach of the Conditions of Computer Use, the University reserves the right to investigate fully, including directly monitoring use of the network and computing facilities by the user. The University also reserves the right to withdraw (either temporarily or permanently) the authority of any user to use any system in such circumstances. Direct monitoring of individual use and/or withdrawal of services in such circumstances may be authorised only by the Director of

Information Services
I.T. & computing

Information Services, or their authorised deputies, in consultation with the Human Resources Division (or the Dean of Students Office in the case of student users).

(b) A breach of these conditions of use may lead to disciplinary proceedings and, in serious cases, dismissal for staff and exclusion for students. (A significant breach of these conditions of use is likely to be regarded as serious or gross misconduct.) A breach of these conditions of use may also constitute a criminal offence and the University will report the matter to the Police where appropriate.

(c) The University reserves the right to charge users for the restitution costs, as determined by the University, in relation to any damage they wilfully cause to any IT facilities.

(d) The University also reserves the right to seek reimbursement of any costs arising from legal actions taken against the University caused by any failure of a user to comply with the requirements of these Conditions of Computer Use, where this has been due to wilful neglect, deliberate avoidance or criminal act.

6. Reporting Computer Misuse

Computer misuse is any activity involving the University's computing resources which is illegal, contravenes these Conditions of Computer Use, or has any of the following characteristics:

- Compromises the security of the University's IT systems or its data.
- Breaches the University's Information Security Policies.
- Results in a formal complaint from a member of the public or another member of the University.
- Is part of a Police enquiry.

If a member of the University becomes aware of such activity, they have a responsibility to report this to either the Information Service's Assistant Director Strategy, Policy and Compliance, or in their absence the Director of Information Services[4]. If appropriate they will initiate any investigative action and will inform and engage with the Human Resources Division, Dean of Students Office and/or head of department as appropriate. All information received will be treated in a confidential manner, only involving other individuals where strictly necessary to any investigation.

A form has been setup on the University's website for reporting misuse:

http://www.uea.ac.uk/is/itregs/misuse.

7. Advice and Clarification

---

[4] Contact information for these people can be found at http://www.uea.ac.uk/is/contacts

Information Services
I.T. & computing

Information Services are responsible for ensuring regular monitoring and updating of these Conditions of Computer Use on behalf of the University.

Should you need any advice and/ or clarification of these Conditions of Computer Use then please contact the IT Helpdesk in the first instance:

- Staff: Tel. 01603 59 2345 or e-mail staff.help@uea.ac.uk

- Students: Tel. 01603 59 3169 or e-mail it.helpdesk@uea.ac.uk

8. Document Review and Communication

Information Services is responsible for the review and communication of these Conditions of Computer Use. There will be an annual mini-review in order to keep up to date with changes in legislation and technology, and a major review every five years[5]. The review will be overseen by a team consisting of representatives from Information Services, the Human Resources Division and the Dean of Students' Office. The IT and Computing Forum, IT support managers, student representatives and staff trade unions will also be consulted as necessary. Revisions to the Conditions of Computer Use will be submitted to the Information Strategy and Services Committee for their consideration and approval as a University policy prior to the start of each academic year.

The Conditions of Computer Use will be published on ISD's website at http://www.uea.ac.uk/is/itregs/usepols and all registered IT account holders will receive an e-mail at the start of the academic year reminding them of the Conditions of Computer Use and their obligations.

---

[5] Last major review was in 2010.

Information Services
I.T. & computing