ISC16D033

University of East Anglia

Title:	**Conditions of Computer Use review**
Author:	Raymond Scott (ISD)
Date:	12 May 2017
Circulation:	ISSC - 13 June 2017
Agenda:	ISC16A003
Version:	2017/18 DRAFT
Status:	Open

Issue

To seek the committee's approval for proposed changes to the Conditions of Computer Use.

Recommendation

Recipients are invited:

- To approve the latest Conditions of Computer Use.

Resource Implications

No change to service is required and therefore there is no impact on resources.

Equality and Diversity

New services will be subject to Equality Impact Assessments as they are implemented.

Timing of decisions

It is intended that the revised Conditions will come into immediate effect once approved by the Committee. They should in any case be in place in time for the start of the 2016-17 Academic Year.

Further Information

- Raymond Scott (ISD), x3561, r.scott@uea.ac.uk

Background

The Conditions of Computer Use are subject to annual review. This paper contains the proposed changes to the policy, which are clearly highlighted.

Conditions of Computer Use

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

Approved by the Information Strategy and Services Committee ~~14 June 2016~~TBD.

Contents

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 loss of access to IT facilities and disciplinary action. 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~~ Service Desk (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.

a) The term **IT facilities** is defined to cover computing equipment such as servers, PCs, laptops, tablets, smartphones and printers; software, data and information held on those systems; information systems used for administrative and other purposes; network access via wired and wireless connections; online services; and the user credentials used to identify you and manage access to facilities.

b) The Conditions of Computer Use apply to all IT facilities owned by the University as well as those owned by third parties for which access has been facilitated by the University. They also apply to personally-owned equipment used to access any of the University IT facilities.

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 MUST 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 and, from May 2018, the General Data Protection Regulation. 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. Staff should not use the University email service for personal (non-work related) emails. 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 whose effect is to bring the University into disrepute. See section 3.4.

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 using approved processes or authorised to do so[1] should install data or software onto University-owned devices and they should ensure it has been checked for viruses or other malware. Where necessary, administrative rights may be granted to permit users to install software on University devices following processes described at https://portal.uea.ac.uk/itservices/security.

Commented [RS(1]: References to GISP may need to be revised should an update to the information security policies be accepted.

i) Do not transmit files/data to others without first checking for viruses or other malware. See section 3.9.

j) 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, have up to date operating system and application software security patches applied and where feasible anti-virus/anti-malware software is installed and is up to date. See section 3.14.

k) All personally-owned electronic devices[2] connected to the network must be registered following processes described at http://www.uea.ac.uk/is/itregs/equipreg. Where a device has been registered using an authorised self-registration process (e.g. in student residences) the

[1] Authorised by the IT or information (data) asset owner. See GISP17 for further details. https://portal.uea.ac.uk/documents/6207125/8136051/GISP17.pdf

[2] In this document, 'device' is used to refer to all equipment which can be connected to the UEA network including PCs, servers, laptops, as well as mobile devices such as phones, tablets and so on. 'Computer' is used to refer to PCs, desktop systems, servers, laptops and notebooks.

owner is responsible for security of that system and any activity on it. Should inappropriate activity be detected arising from the device, 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 where feasible up to date anti-virus/anti-malware software is installed. See section 3.10.

l) 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 misuse and in support of the University's obligations under anti-terrorism legislation. In cases where illegal activity is involved copies of relevant information may be handed to the Police. See section 4.

3. Conditions of Use

3.1 Access to University IT facilities

Use of the University's IT facilities is restricted to the following registered users authenticating by means of a UEA IT account:

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.

Access to specific IT facilities is authorised by the facility owner.

Limited access to the University's IT facilities is available to users authenticating by other means such as eduroam.

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 https://www.uea.ac.uk/is/strategies/User-Entitlements-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. It is the responsibility of the University to ensure that its members use Janet services in accordance with their AUP and current legislation. Further information is available from http://www.uea.ac.uk/is/itregs/legislation.

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.

v. Any other lawful activity in furtherance of the mission of the University.

b) Limited use of the University network and IT facilities for personal purposes other than UEA work or study, for instance 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 purposes[3]) offensive, obscene or indecent data or images, or data from which such material could be derived, or material that might be subject to the provisions of counter-terrorism legislation[4]. The University has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT", to have a due regard for the need to prevent people from being drawn into terrorism.

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

d) Creation or transmission of material with the intent to defraud.

e) Creation or transmission of defamatory, discriminatory or libellous material, or material whose effect is to bring the University into disrepute.

f) Transmission (including downloading, uploading, and streaming) of material that infringes the copyright of another person.

g) 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.

---

[3] Lawful purposes include approved teaching or research, or in the course of an investigation by authorised personnel into suspected abuse of University facilities.

[4] Where academic use is likely to include such material, authorisation should first be sought from the Head of School and the relevant research or ethics committee and the Information Services Assistant Director Strategy, Policy and Compliance made aware. Consultation with external authorities may be required and is advisable under certain circumstances depending on the nature of the activity. In particular, all use of material subject to counter-terrorism legislation shall be used only in accordance with the Counter-Terrorism and Security Act 2015 and the guidance applying to higher education institutions in England and Wales. Security sensitive material shall be handled following UUK guidance http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/oversight-of-security-sensitive-research-material-in-uk-universities.aspx.

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

i) Transmission of unsolicited commercial or advertising material either within the University or externally, unless authorised to do so on behalf of the University and where that material relates to a service to which the recipient has subscribed.

j) Unauthorised access or attempting to gain unauthorised access to IT facilities or services both within and outside the University[5].

k) Disclosing your UEA password to others, or letting others use your UEA IT account[6], 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.

l) Deliberate activities having or likely to have 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. Causing annoyance to others by inappropriate or inconsiderate use of computing facilities (e.g. internet phones in IT areas).

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

   vi. Denying service to others.

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

   viii. Other misuse of University IT facilities or resources, such as the introduction of malicious software, in such a manner that it compromises the security of University systems and the network.

(b) Where the University network is being used to access another network, any deliberate or persistent breach of the acceptable use policy of that network.

---

[5] The University may perform authorised vulnerability tests on its IT systems. Any such external tests must be reported in advance to Janet CSIRT.

[6] Where an individual is absent from work for a prolonged period, or leaves the institution without first passing on their digital assets 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. (When a member of staff leaves, their account is frozen, and deleted 100 days after their contract end date.)

3.5 Data protection and privacy

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, be accurate and up to date, stored securely for no longer than needed to fulfil its stated purpose and not disclosed to any other person unlawfully.

a) Individuals have a right of access to their own personal data, and staff must comply without undue delay with any data requests received from the Information Policy and Compliance Managers (dataprotection@uea.ac.uk).

b) The University reserves the right to remotely extract relevant information from emails and other filestores where necessary to comply with our legal obligations. This will be handled in accordance with an agreed search protocol.

~~a)~~c) 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 and General Data Protection Regulation (GDPR).

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

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

~~d)~~f) Those in the University who have data in their care, or who are authorised by the University to process personal data must complete online data protection training and ensure that they are aware of their obligations under ~~the Data Protection Act~~ privacy legislation to comply with the d~~D~~ata p~~P~~rotection principles~~. These principles along with more information about the Act and its applicability at UEA can be found~~ at https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/data-protection. In particular, handling, sharing and the removal of personal data from the University should be minimised. Encryption must be used when taking personal data off site by any means including use of mobile devices (including laptops), removable storage or emails to external email addresses to avoid the possibility of inadvertent and unintended disclosure to unauthorised third parties (the seventh data protection principle). Personal data must be transmitted or transported off campus only in an encrypted form.[7]

~~e)~~g) If you share personal data with third parties external to the University, a data sharing agreement must be in place to govern the sharing. Contact the Information Policy and Compliance Managers for advice (dataprotection@uea.ac.uk).

~~f)~~h) Where users have data in their care relating to University research, teaching or administration, they should also be aware of and comply with the following:

[7] Further information on encrypting data sent by email is available at https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/data-protection/data-protection-act-faqs#Q.18

i. The University's General Information Security Policy - see https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/information-security/gisp.

ii. All 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 Management Policy. See http://www.uea.ac.uk/is/strategies/infregs/Information+classification+policy.

~~ii.~~iii. All losses of personal data or devices containing personal data including removable storage and media must be immediately reported to the information compliance team at dataprotection@uea.ac.uk. See https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/data-protection/data-breaches ~~dataprotection@uea.ac.uk. See~~

~~g~~)i) 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.

~~h~~)j) Users using devices configured to synchronise with or link to any University IT service (such as the Exchange server or filestore) must set security on the device to prevent unauthorised access. Staff using their own personally-owned devices for conducting University business including receipt of emails should ensure that the devices and the data held on them are secured to the same standard as defined in the University's information security policies.

~~i~~)k) Users should not root or jailbreak (i.e. circumvent the security) any University-owned devices. Devices operated in this state are liable to be more easily compromised. Any attempt to bypass the security built into a device is potentially an offence under the Computer Misuse Act 1990.

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. All University staff, particularly those with responsibilities for recorded information, should therefore be aware of and follow the guidelines at https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/freedom-of-information/guidance-for-staff, and note that FOIA applies to all recorded information held electronically or in physical form including documents, records, notebooks, voicemails, videos, photos and emails.

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

Commented [RS(2]: References to GISP may need to be updated should revision to information security policies be accepted.

scanning, recording, streaming, and downloading, and covers print, digital and web-based material.

b) Copyright material should not be networked or otherwise shared with 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 https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/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 must only be used in accordance with licence conditions of the software. You must 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.

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) Software provided by the University should not be installed, removed, disabled or altered, other than by approved methods.

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

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

h) 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 means of a Username and Password.

b) 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 GISP5 of the General Information Security Policy at https://portal.uea.ac.uk/documents/6207125/8136051/GISP5.pdf. Passwords must be changed at least every 12 months to maintain security.

Commented [RS(3]: References to GISP may need to be updated.

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

d) All devices connected to the University's campus wired network must run a currently supported operating system. "Currently supported" means within the product lifecycle, i.e. the operating system must have been released, not preview or beta, and still be in receipt of security patches from the software vendor. All devices should have up-to-date operating system and application software security patches applied and where feasible anti-virus/anti-malware 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 Services' recommendations with auto updating enabled and following ~~guidelines and~~ policies defined in the General Information Security Policy.

e) Only those authorised to do so[8] should install data or software onto University-owned devices and they should ensure it has been checked for viruses or other malware. All installed software must be securely configured according to Information Services' recommendations and following ~~guidelines and~~ policies defined in the General Information Security Policy. Where necessary, administrative rights may be granted to permit users to install software on University devices following processes described at https://portal.uea.ac.uk/itservices/security. Users should not transmit files/data to others, without first checking for viruses or other malware.

Commented [RS(4]: Reference to GISP may need to be updated.

f) Information Services reserves the right to disconnect any computer from the network that is discovered to be infected with malware (e.g. viruses, trojans), that is suspected of being compromised or being involved in activities in breach of these Conditions of Computer Use, or which does not have adequate virus-checking software installed. The associated password should be reset on an uninfected machine. Once cleaned, the device can be reconnected to the network.

3.10 Connecting equipment to the network

a) All devices connected to the University's network must follow the University approved policies and processes detailed at http://www.uea.ac.uk/is/itregs/equipreg.

b) No equipment connected to the network (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 or registered using self-registration processes detailed at http://www.uea.ac.uk/is/itregs/equipreg must

[8] Authorised by the IT or information (data) asset owner. See GISP17 for further details. https://portal.uea.ac.uk/documents/6207125/8136051/GISP17.pdf

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 device will be held responsible for any inappropriate activity arising from that device[9]. In the case of personally-owned systems the owner is responsible for ensuring that the device has up to date operating system and application software security patches applied, and where feasible (i.e. where such software is available) 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[10].

b) Staff must regularly access their UEA e-mail account mailbox to manage any received correspondence.

c) Where practical, staff should not use University e-mail systems for sending personal messages unrelated to University matters[11].

d) 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://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-guidelines.

e) The ~~Data Protection~~DPA/GDPR and Freedom of Information Act~~s~~ also apply to e-mails. Such e-mails must be stored and processed in accordance with the ~~Data Protection Act~~DPA/GDPR and may have to be released in response to Freedom of Information Act requests, and requests made under the DPA and GDPR. For more information on these Acts see sections 3.5 and 3.6.

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

g) 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

[9] 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.

[10] In cases where a member of UEA staff is working in another associated or affiliated institution for a significant period of time, and where they wish to have access to their UEA emails from within their mailbox provided by that institution, requests for automatic forwarding of UEA emails will be considered by Information Services.

[11] Staff wishing to send or receive personal ~~e-mail~~email messages whilst at work should use a web-based external email service such as those provided by Google, Yahoo, or Microsoft etc.

detailed at http://www.uea.ac.uk/password and should be communicated to the intended recipient by other means.

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

i) 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 https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/user-guidelines.

j) Only a user's UEA assigned ~~e~~e-mail address will be used to send e-mail messages from the University to the user. Undergraduate and ~~post graduate~~postgraduate (PGT and PGR) students 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.

k) 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'.

l) Files downloaded from the internet, including mobile code[12] and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

3.12 Internet publishing

The University adheres to principles of academic freedom of expression. However, those publishing information via the internet should note the following~~.~~:

a) Users should be aware that posting information to any extended group including but not limited to discussion forums, websites, social media sites, news feeds 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 to the general public via the internet is considered to constitute its publication.

[12] Programs, often in the form of scripts or applets, which are downloaded across the network and run on a local machine are often referred to as mobile code.

b) No item should be published using the University's IT 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 or request the removal of any such material and to remove access rights in order to prevent further publishing of such material.

c) Students are advised to consult the guidance on the use of social media published by the Student Support Service [13].

d) Staff and those with comparable honorary status are advised to consult the code of conduct on social media use published by HRD which outlines the standards expected for safe, professional and appropriate online behaviour.[14]

e) Any social media accounts and blogs affiliated to the University must follow policy[15] and take note of guidance[16] published by the University Marketing Team, and should be confirmed and registered with the Social Media Co-ordinator via tweet@uea.ac.uk as soon as they are created.

f) Before creating a new website affiliated with the University, the user must consult the Digital Innovation Team at digital@uea.ac.uk and follow guidance and advice given to be compliant with UEA policy. (Domain registrations will be considered and approved by the Digital Innovation Team and set up and administered by ISD via digital@uea.ac.uk.)

g) 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.

h) 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.[17]

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

---

[13] https://portal.uea.ac.uk/student-support-service/student-conduct-and-harassment~~https://portal.uea.ac.uk/dos/student-conduct-and-harassment~~

[14] https://www.uea.ac.uk/hr/employee-information/policies/social-media-conduct

[15] https://portal.uea.ac.uk/documents/6207125/10820892/UEA+staff+social+media+policy+FINAL.pdf

[16] https://portal.uea.ac.uk/arm/marketing/social-media

[17] https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/it-regulations-and-policies/user-guidelines/email-disclaimer-notice

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 which includes non-commercial use only. Copies of these licences, which include full details of copyright restrictions, are available for inspection on application to the Main Library.

c) The University is not liable for any financial or material loss to an individual user in accessing the internet for personal use. In particular, 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 circumstances as described in Section 4 apply, or 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 reset or divulged to others, except:

i. Where a reset 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 department should contact the Service Desk, who will request the completion of an IT account access authorisation form. 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 must 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 must 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 connect 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 beare published on the Procurement web pages (https://portal.uea.ac.uk/procurement).

Commented [RS(5]: Do we have a link to details on this service?

Commented [RS(6R5]: Asked MJ to provide a link. Or the reference to the link should be removed.

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[18] 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

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

those systems. Policies and controls as detailed in the ~~General Information Security Policy and in the Security Manual~~General Information Security Policy 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.

3.15 Visitors

The Conditions of Computer Use as they apply to visitors to the University may be summarised as follows:

a) Visitors must not intentionally contravene these University Conditions of Computer Use in any way.

b) If residing in University residences, visitors must not contravene the Self-Registered Equipment Terms and Conditions at http://www.uea.ac.uk/is/itregs/selfregtc

c) A visitor's IT equipment must not be used on the University network without having been registered for such or authenticated via eduroam.

d) A visitor's computer must not be connected to the University network without up-to-date anti-virus/anti-malware software being installed and operational.

e) Visitors must not attempt to run any software whose use is prohibited by the University, either on their own system connected to the University network, or on University-owned systems.

f) Visitors must not disclose to anyone else passwords which have been allocated to them for the purpose of authorised access to University IT and computer systems.

g) Visitors must not take any action to circumvent any University security control that is in place.

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, enforcement of these Conditions of Computer Use, and in support of the University's obligations under anti-terrorism legislation to prevent people from being drawn into terrorism. Monitoring may reveal to operational staff unencrypted data and sites visited by users. 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 IT 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 process

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 determine the dates when email, network and the campus card were last used in support of the missing person's protocol.

iii. 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.

iv. In the course of an investigation triggered by indications or allegations of misconduct, misuse, or illegal activity reported by managers or colleagues, monitoring processes, or some other legitimate and objective complaint or incident.

v. To respond to legal processes such as requests for information under FOIA or data protection, or to fulfil the University's obligations to third parties or in other exceptional circumstances, e.g. medical emergency.

vi. Electronic correspondence will only be intercepted in exceptional circumstances, and only with lawful authority.

d) All access and monitoring will be undertaken in accordance with the Human Rights Act 1998, Data Protection Act 1998, General Data Protection Regulation (from May 2018), Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the Regulation of Investigatory Powers Act 2000.

Commented [E(7]: Add text about remote searching of accounts in specific circumstances?

Commented [RS(8R7]: This section starts with 'University reserves the right to process information stored on University IT system under the following circumstances'. I think it is telling users when we will waive their right to privacy on UEA systems already.

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, or their authorised deputies, in consultation with the Human Resources Division (or the Student Support Service in the case of student users).

b) A breach of these conditions of use may lead to disciplinary proceedings and/or disconnection from the data network. In serious cases, this could result in dismissal for staff or 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 IT facilities 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[19]. If appropriate, they will initiate any investigative action and will inform and engage with the Human Resources Division, Student Support Service 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~~There is a form on the University's website for reporting misuse:

https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/it-regulations-and-policies/report-computer-misuse.

7. Advice and Clarification

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~~ Service Desk in the first instance:

- Tel. 01603 59 2345 or e-mail it.servicedesk@uea.ac.uk

[19] Contact information for these people can be found at https://portal.uea.ac.uk/information-services/contacts.

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[20]. The review will be overseen by a team consisting of representatives from Information Services, the Human Resources Division and the Student Support Service. 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.

[20] Last major review was in 2015.