

Produced by CCSS and Human Resources

August 2018

Human Resources Policy Statement HRPS36

Computer Use Policy for Staff

Introduction

This Policy explains:

- how you as a person working in the capacity of a University staff member ("**Users**") may use the University's computing facilities;
- how Users or the University may be liable in law for misuse of the University's computing facilities;
- how User's interests and the University's interests can be protected;
- the action which may be taken against Users if you fail to comply with the rules and regulations set out in this Policy; and
- details of the email and file storage services provided by Microsoft.

Background

The University encourages all Users to use the University's computing facilities as tools to assist their work; Users have no right to use the facilities for any other purpose. However, the University's computing facilities may only be used in accordance with this Policy. Any use of the University's computing facilities which use the electronic communications network used by the UK education and research community known as the Joint Academic Network ("JANET") is also subject to the JANET Acceptable Use rules. Users hereby agree to abide by these additional rules where applicable and to the extent relevant. These rules can be read by clicking here: <https://community.jisc.ac.uk/library/acceptable-use-policy>.

You hereby agree to use the Middlesex Staff Office365 and OneDrive facilities (together, the "**Microsoft Facilities**") as provided by Microsoft on behalf of the University in accordance with these terms and conditions and you hereby agree that you are also bound by Microsoft's

Terms Of Use' which can be read by clicking here: <https://www.microsoft.com/en-us/legal/intellectualproperty/copyright/default.aspx>.

The University reserves the right to amend any of the rules set out in this Policy at any time, and will notify all Users of any changes it makes.

This Policy applies to all computer users within the University (including persons who are classified as non-core staff but who have been authorised in writing by the University to use the University's computing facilities, e.g. agency, partner, contractor, etc.), whether they use computers based at the University's premises or access the systems provided by the University via the internet using University-owned or private computing equipment. Compliance with this Policy does not imply authorisation to use the University's computing facilities.

In accordance with User's contract of employment (or work order) with the University, the 'University Grievance & Disciplinary Procedures' and the 'Staff Handbook' (together, the "**Staff Regulations**"), the University considers failure or refusal to comply with this Policy to be a serious disciplinary offence which may lead to disciplinary action including withdrawal of services, and/or dismissal without notice.

When using the University's computing facilities Users must conduct themselves, at all times, in a lawful and appropriate manner so as not to discredit or harm the University or other Users and at all times in accordance with the contents of this Policy. Accordingly, this Policy is not a definitive statement of the purposes for which the University's computing facilities should or should not be used and the University reserves the right to apply this Policy in a purposive manner.

The University's computing facilities are provided to assist with day to day work. Personal and recreational use is allowed; however, the University accepts no responsibility for personal data stored on devices or storage facilities. The University also reserves the right to place whatever limitations it deems appropriate on such usage in order to safeguard the function of its computing facilities and Users' compliance with any applicable laws and/or the contents of this Policy.

Basic Rules

- i) Only use the University's computing facilities for lawful activities. The University will not hesitate to contact the police if it discovers unlawful use of University computing facilities.
- ii) Do not engage in any activity or omit to do anything which could jeopardise the integrity or security of the University's computing facilities.
- iii) Keep your Network Identity, all your User Accounts and associated passwords secure.
- iv) Do not share your own or use someone else's Network Identity and User Account.
- v) Managers may only access a User's account in their absence where the User has given their explicit approval. Approval should be sought from Human Resources where access to the User's account is required to ensure continuity of business services and where every reasonable effort has been made to seek the User's permission, but it has not been possible to contact the User.

- vi) Prior to leaving the University, Users are required to delete or arrange the transfer of all files and emails from their account. The University reserves all rights to access a leaver's emails and files for the purposes of ensuring the smooth continuity of business services.
- vii) Do not use, or permit others to use, the University's computing network for any commercial use, nor for the purposes of endorsing or advertising such activity without the express authority of the University's IT Department, currently known as the Computing and Communications Systems Service ("CCSS").
- viii) Do not alter, interfere, add to or remove any physical part of the University's computing facilities or any equipment connected or attached to the University's computing facilities without authorisation. Data points provided for Users are designed to support one computer only and the unauthorised connection of hubs and switches to data points is forbidden.
- ix) Do not access material, or attempt to access material, that you do not have permission to access.
- x) Do not bypass the login procedure.
- xi) Do not deny (or do anything which has the effect of denying) another Users' legitimate access to the University's computing facilities.
- xii) Do not connect any server, modem, wireless routers and hubs or network routers / switches / hubs to the University's computer network, or other similar transmitting device that operates on a wireless frequency without prior written agreement from CCSS.
- xiii) Do not make, store or transmit unlicensed copies of any trademark or copyrighted work (including software and media files).
- xiv) Do not send unsolicited bulk email messages, chain mail or spam.
- xv) Do not deliberately or recklessly undertake activities which may result in any of the following:
- The waste of other Users' efforts or network resources, including time on any system accessible via the University network
 - The corruption or disruption of other User's data
 - The violation of the privacy of other Users
 - The disruption of the work of other Users
 - The introduction or transmission of a virus into the network

Unauthorised Use of the Internet

- i) Do not, other than for ethically cleared, properly approved and lawful research purposes (as set out below) visit, view, store, download, transmit, display, print or distribute any material relating to:
- Sex or pornography;
 - Lewd or obscene material of any nature or other material which may be likely to cause offence to another person;

- Terrorism or cults;
- Hate sites (racial or other).

Users seeking authorisation for the above (for 'ethically cleared, properly approved and lawful research purposes') must obtain prior written approval from their Dean of School or the appropriate member of the Executive and this approval needs to be reconfirmed in writing every 6 months. In addition, Users should not intentionally do anything which enables others to visit, view, download transmit, display, or distribute any material relating to the items listed above.

ii) Do not attempt to gain unauthorised access to any facility or service within or outside the University, or make any attempt to disrupt or impair such a service.

iii) Do not setup or use hardware, or software, on the University's own internal network (and not, for the avoidance of doubt, JANET) for the purpose of sniffing, hacking, network scanning or keyboard logging without prior written authorization.

iv) Do not alter or interfere with data, programs, files, electronic mail or other computer material which you do not have the right to alter.

v) News Groups, Web Sites, Wikis, Blogs:

- Do not post or present information in such a way as may bring the University into disrepute or otherwise damage the reputation of the University.
- Do not express opinions which purport to be the University's view unless you are authorised in writing to express views on behalf of the University.
- Do not distribute or share group members' user names, email addresses and other personal information with non-group members, unless explicit permission has been granted.
- The University reserves the right to approve and withdraw approval of any News and Community Group, Web Site, Wiki and Blog.

In accordance with the Staff Regulations, any transgression or breach of the above restrictions or policies will be deemed as gross misconduct which may result in summary dismissal of staff and/or withdrawal of services following a proper hearing of the case. Users will be held responsible for any claims brought against the University in respect of any legal action to which the University is, or might be, exposed as a result of User's misuse of the University's computing facilities, including reimbursing the University for any financial liability which the University suffers as a result of a User's actions or omissions. The University will not hesitate to contact the police if it discovers unlawful use of the University's computing facilities.

Unintentional Access to Inappropriate Internet Sites:

The University accepts that mistakes can be made due to unintended responses of search engines, unclear hypertext links, misleading advertisements and typing errors taking Users to

inappropriate web pages.

Email

The University encourages Users to use email as a prompt and effective method of communication.

Email services are provided to Users primarily for bona-fide business purposes, although limited personal use is allowed. The University reserves the right to place whatever limitations it deems appropriate on such usage in order to safeguard the primary function of its own network (not, for the avoidance of doubt, JANET).

Email services are provided to Users through the use of Microsoft's Facilities.

Users must act responsibly and appropriately when using the University's computing facilities to send email, whether internally or externally using the Internet.

No User should send email that contains material that the University considers or might reasonably be considered by the recipient as offensive, (including without limitation bullying, harassing, discriminatory, pornographic, homophobic, excessively violent, obscene, blasphemous, seditious, incite racial hatred), defamatory or in any way break any law relating to published material or which contains any malicious code; for example a virus. If you receive an email containing any such material, and you are concerned about this you should inform your Line Manager.

Users must not send email which might bring the University into disrepute or purport to be the view(s) of the University unless the User is authorised in writing to express views on behalf of the University.

The University and the University on behalf of its externally hosted providers, including Microsoft, reserves the right to automatically delete emails which are found to contain viruses or constitute a data security breach (e.g. contain sensitive and or authentication cardholder data). The University endeavours to protect Users from offensive emails through the operation of 'Anti Spam filters' (as part of the Microsoft Facilities) PROVIDED THAT in addition, Users endeavour to reduce the amount of offensive material they receive by the configuration of their email setup to screen out and delete unwanted emails.

Users hereby agree that emails generated by, or stored on, the University's computers may be subject to disclosure under the Freedom of Information Act and Data Protection Act as well as potentially dis-closable and admissible in evidence, in a dispute.

Legitimate Use

There may be circumstances where a User feels that the nature of their work or studies means they have a legitimate reason for accessing and/or using material prohibited under this Policy. In this circumstance the User must discuss this with their Line Manager in advance as to the precise reasons for such access and use and no such access and/or use may be undertaken without the express written approval of the Line Manager. If the Line Manager is in doubt they must contact CCSS for advice.

Software

Unauthorised Software:

The University will take disciplinary action against any User who acquires, uses or distributes unauthorised copies of any software using the University's computing facilities.

Introducing Software:

Users are prohibited from using any software on the University's computing facilities which the User and/or the University is not licensed to use.

Educational Use Licences:

The University licenses computer software from a variety of outside sources and many software packages are licensed only for educational use. The University does not own this software or related documentation and, unless authorised by the software owner, does not have the right to reproduce it. The software used on the local area network or multiple/individual machines may only be used in accordance with the relevant licence agreement and in no circumstances for any commercial use without the express authorisation of CCSS.

CHEST Software:

Software supplied by CHEST (Combined Higher Education Software Team) is subject to the CHEST Code of Conduct for the Use of Software and Datasets. Users are bound by that Code of Conduct, which should be read by clicking here <https://www.chest.ac.uk/Chest-Agreements/about-our-licences/user-obligations>

Distribution of Software:

Users are prohibited from using the University's computing facilities to distribute software unless (and not without the University's express written approval) it is directly associated with the University's business and where such distribution does not contravene any other part of this Policy.

Suspected Misuse:

Users should immediately notify CCSS of any misuse or suspected misuse of software or associated documentation.

US Export Law

Users hereby acknowledge that much of the software and hardware provided by the University for their use is produced and developed by suppliers based in the United States of America and therefore governed by US Export Law. Staff travelling to countries defined by the US Department of Commerce as "embargoed countries" should check with CCSS before taking University hardware and software abroad with them. Further information on the list of embargoed countries can be found at the Bureau of Industry and Security web site: <https://www.bis.doc.gov>. Countries currently on the embargoed list are: Cuba, Iran, Sudan, Syria and North Korea.

Security and Viruses

It is each User's responsibility to log off from the system, when leaving the computer being used, to avoid inadvertent security breaches.

Users must not disclose (including by sending via or placing on the Internet) any material, which incites or encourages or enables others to gain unauthorised access to the University's computer facilities.

It is vital that all Users take all necessary steps to safeguard the University's computer facilities from viruses. Accordingly, all Users using personal computers on JANET must ensure that antivirus software is installed on their desktop / laptop computer and kept up to date and that any unsolicited documents or attachments received are deleted immediately.

Offensive or Defamatory Material

Emails and the Internet are considered to be a form of publication and therefore the use of the Internet, email and the making available of any information online, must not be offensive, (including without limitation bullying, harassing, discriminatory, pornographic, homophobic, excessively violent, obscene, blasphemous, seditious, incite racial hatred), defamatory or in any way break any law relating to published material. Misuse of email or inappropriate use of the Internet by viewing, accessing, transmitting or downloading any such offensive information will amount to gross misconduct in accordance with the Staff Regulations and may result in summary dismissal and/or withdrawal of services.

Words and pictures produced on the Internet are capable of being defamatory if, for instance, they are untrue, ridicule a person and as a result damage that person's reputation. For these purposes, as well as any individuals, a "person" may include the University or another institution. You must not create or transmit any statement which may be offensive or defamatory in the course of using the Internet or the University's computing facilities whether in emails or otherwise. As well as you being personally exposed to potential legal action for defamation, the University and JANET as the 'Internet Service Provider' would also be held liable.

Obscenity

It is a criminal offence to publish or distribute obscene material or to display indecent material in public. The Internet or any computer 'message boards' qualify as a public place. The accessing or sending of obscene or indecent material using the University's computing facilities is strictly forbidden and in accordance with the Staff Regulations may result in summary dismissal and/or withdrawal of services.

Discrimination and Harassment

The University does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed on the University's computing facilities or via the Internet. Users should not view, use or distribute any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender,

sexual orientation, gender reassignment, marital status, age, ethnic origin, colour, nationality, race, religion, belief or disability.

Data Protection

Any work involving processing, storing or recording personal data (information on an identifiable living individual) is governed by the Data Protection Act 2018. It is the User's responsibility to ensure that personal data is collected and used in accordance with the Act. Further information can be obtained from the University's Data Protection Policy. If you believe that your work involves the processing, storing or recording of personal data, Users must first obtain confirmation from the Data Protection Officer that consent to such processing, storage or recording has been obtained.

Third-Party Data Storage/Cloud Services

Staff wishing to store University data on storage provided by an external third-party often referred to as "in the cloud" need to make sure such data storage is in accordance with the University's Data Protection Policy. In addition a contract with the third-party needs to be put in place to provide the University with adequate legal safeguards as to the confidentiality, integrity and availability of the data. Most staff will not have the authority to bind the University to such a contract and will need to refer the matter to someone who does.

In addition to these considerations, staff using the service must ensure that data is transferred to/from the cloud in a secure manner and that access is restricted to authorised personnel. The contract with the cloud service provider may provide for backing up of the data but if not then the staff using the service must make adequate provision to provide a secure backup of the data. A Middlesex owner of the Data stored on the external site should be formally identified who will be responsible for authorising and maintaining access to the data. Arrangements should also be put in place to formally pass on this responsibility if the current owner should leave the University. Data should be stored only as long as it is needed in accordance with the University, School and Service data retention policies. Hence staff must setup procedures to remove data from the cloud service when it is no longer required.

Some cloud services are provided on an individual basis and hence the data may need to be removed if the personnel involved are no longer members of the University.

This is a complicated area and staff are advised to contact CCSS before proceeding.

Monitoring

The University reserves the right without notice to monitor Users' use of the University's computing facilities and to access data held on the University's computing facilities for justifiable business purposes and in order to perform various legal obligations including:

- where it is suspected that a User is misusing the University's computing facilities;
- to investigate misuse of the University's computing facilities;

- where the University has received a request from an authorised external party to monitor a User's use of the University's computing facilities;
- to prevent or detect crime (including 'hacking');
- to prevent or detect data security breaches;
- to resolve system performance problems which may otherwise damage the computing services provided to other University users; or
- to intercept emails for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding emails to correct destinations.

The University reserves the right to automatically block certain network protocols and sites in order to minimise the risk of viruses, hacking, network scanning and other inappropriate file transfer activities.

The University maintains logs of user and network activity which may be used in investigations of breaches of University computing regulations, performance monitoring or provision of statistical reports.

The University has a statutory duty under Section 26(1) of the Counter-Terrorism and Security Act 2015 ("the Act") when exercising its functions, to have due regard to the need to prevent people from being drawn into terrorism. The University may impose filtering and/or monitoring, as required in its view, to support this duty.

Users should be aware that the CCSS has adopted a formal Investigations Procedure which will be instigated where the University reasonably suspects misuse of the facilities or breach of this Policy.

The University reserves the right to make and keep copies of emails and data documenting use of email and/or the Internet systems, for the purposes set out above.

Users hereby acknowledge and agree that the University has the right to retain copies or delete copies of any data stored on the system so as to comply with the University's statutory obligations or, at its own discretion, in accordance with the legitimate purposes stated above.

In using the University's computing facilities, Users implicitly accept this Policy. Consequently Users agree to their activities being monitored in the circumstances given above.

Availability

Users acknowledge that the University's computing facilities may not be available for 24 hours 7 days a week. The University retains the right to limit or prevent access to the University's computing facilities for the purposes of carrying out planned or unplanned maintenance, virus monitoring and/or clean up or investigation. Except where the University cannot exclude or limit its liability as a matter of law, the University shall have no liability to any User in connection with the non-availability of the University's computing facilities howsoever arising, including in negligence.

Liability for Misuse and Disciplinary Action

Civil and Criminal Liability:

Users and the University are potentially at risk for a range of civil and criminal liability arising from misuse of the University's computing facilities. Legal liability can arise from:

- defamation under the **Defamation Act 2013**;
- copyright infringement under the **Copyright, Designs and Patent Act 1988**;
- breach of confidence;
- negligent virus transmission;
- computer hacking and any breach of the **Computer Misuse Act 1990** and the **Police and Justice Act 2006**;
- breach of the **Obscene Publications Acts of 1959 and 1964**, the **Protection of Children Act 1978** and the **Telecommunications Act 1984** and the **Communications Act 2003**;
- harassment and discrimination under the **Equality Act 2010**, the **Racial and Religious Hatred Act 2006** and the **Malicious Communications Act 1988**;
- the **Data Protection Act 2018** and the **Human Rights Act 1998**;
- the **Investigatory Powers Act 2016**, the **Privacy and Electronic Communications Regulations 2003**, the **Terrorism Act 2006**, the **Serious Organised Crime and Police Act 2005** and the **Counter-Terrorism and Security Act 2015**.

Misuse of the University's computing facilities (including failing to comply with this Policy) may expose both Users personally and/or the University to court proceedings attracting both criminal and civil liability. Users will be held responsible for any claims brought against the University for any legal action to which the University is, or might be, exposed as a result of User's misuse of the University's computing facilities including reimbursing the University for any financial liability which the University suffers as a result of Users actions or omissions.

The University considers failure or refusal to comply with this Policy to be a disciplinary offence which may lead to disciplinary action taken including dismissal without notice and/or withdrawal of services. Action will be taken in accordance with the Staff Regulations

Users acknowledge that it is their own responsibility to create and maintain 'back-ups' of any data. The back-ups taken by the University are used for systems recovery purposes and only in exceptional circumstances will CCSS recover a Users' files and emails.

The University's Liability to Users:

The University does not exclude its liability under this Policy (if any) to Users:

- for personal injury or death resulting from the University's negligence;
- for any matter which it would be illegal for the University to exclude or to attempt to exclude its liability; or

- for fraudulent misrepresentation.

Except as provided above, the University will be under no liability to Users whatsoever (whether in contract, tort (including negligence), breach of statutory duty, restitution or otherwise) for any injury, death, damage or direct, indirect or consequential loss (all three of which terms include, without limitation, pure economic loss, loss of profits, loss of business, loss of data, loss of opportunity, depletion of goodwill and like loss) howsoever caused arising out of or in connection with the use of the University's computing facilities.

This Policy is governed by the laws of England and Wales and is subject to the non-exclusive jurisdiction of the English Courts.