# *Student Acceptable Use Policy*

*Policy Owner: Business Development Director*
*Last Updated: Aug 2016*
*Last Reviewed: Feb 2017*
*Next Review Date: July 2017*
*Version Number: v1.1*
*Informed by Quality Code Chapters:*

*Student Acceptable Use Policy*

*Applicable to students using ICMP ICT systems*

*Related Polices:*

- **Data Protection Manual**
- **Social Media Policy**
- **Equality & Diversity Policy**
- **Safeguarding Policy**

1. *Definitions*
   - **1.1. "***ICT Systems***" includes:**
     - **1.1.1. central services as provided by ICMP such as e-mail, networks, internet access, computers, computing equipment and mobile devices;**
     - **1.1.2. personally owned computers, mobile devices and peripherals when connected to, or accessed from or via ICMP facilities referred to as 'Bring Your Own Device" (BYOD);**
     - **1.1.3. use of remote networks and services, when accessed from or via ICMP ICT Systems;**
     - **1.1.4. all programmable equipment; any associated software and data, including data created by persons other than users, and the networking elements which link ICT Systems.**
   - **1.2. "***users***" includes students and any other person authorised to use ICMP's ICT Systems.**
   - **1.3.** ***"connected to"*** **means connected either physically or virtually.**
   - **1.4. "***files***" include data and software but do not include manual files.**

2. *Purpose and scope*
   - **2.1. This policy sets out the standards which apply to students in their use of our ICT Systems including personal devices collectively referred to as BYOD.**
   - **2.2. Our ICT Systems are provided to users as part of their equipment for work and/or study, namely for learning, training, research, development and administrative purposes. There are, however, risks involved in the use of the ICT Systems. Inappropriate use of the Internet or e-mail could damage the operation, business or academic activities or reputation of ICMP. Examples of such risks include:**
     - **2.2.1. claims brought against ICMP because the reputation of other individuals or organisations has been damaged;**
     - **2.2.2. infringement of copyright, licenses and other rights in ICMP's and other parties' material (which includes infringement arising from the use of material without the permission of the author);**
     - **2.2.3. harassment and discrimination claims being brought against ICMP (caused by offensive or other inappropriate material);**
     - **2.2.4. the introduction of viruses to ICMP's ICT Systems.**
   - **2.3. This policy is designed to prevent these and other problems and therefore you are expected to be familiar with and comply with the contents of this policy. Users should seek advice and clarity if unsure about whether anything they are considering undertaking might breach this policy.**
   - **2.4. Failure to adhere to this policy may result in disciplinary action, ranging from revocation of network access to withdrawal from your programme of study.**
   - **2.5. This policy applies to all users in whatever location they are working whether or not on our premises.**

**2.6. This policy takes into account the current legal position but users should be aware that it will continue to change, often at great pace. For this reason, all users must ensure that they update themselves regularly with this policy. In the event of a conflict between this policy and the law the law will prevail.**

3. *Bring Your Own Device (BYOD)*

**3.1. The ICMP recognises the benefits that can be achieved by allowing users to use their own electronic devices. ICMP must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing.**

**3.2. Users who make use of BYOD must take responsibility for their own device and how they use it. They must:**

**3.2.1. familiarise themselves with their device and its security features so that they can ensure the safety of ICMP information as well as their own information;**

**3.2.2. invoke the relevant security features;**

**3.2.3. maintain the device themselves ensuring it is regularly patched and upgraded;**

**3.3. All users using BYOD must take all reasonable steps to:**

**3.3.1. prevent theft and loss of data;**

**3.3.2. keep information confidential where appropriate;**

**3.3.3. maintain the integrity of data and information, including that on campus;**

**3.3.4. take responsibility for any software they download onto their device.**

4. *Disabled Students and Staff*

**4.1. The IT systems in use are regularly reviewed to ensure they are DDA compliant. Please refer to our Access Statement or contact ICMP Students Services for further information on the services we provide to disabled people.**

5. *Usernames and passwords*

**5.1. You should keep your password secure at all times and must not reveal your password to anyone else. The use of another person's username and/or password, with or without their permission will be dealt with under Student Disciplinary Procedures as appropriate.**

**5.2. Your password must conform to the following password policy:**

**5.2.1. Passwords must be at least 8 characters long.**

**5.2.2. Passwords cannot contain your name or user name**

**5.2.3. Accounts are locked out after 6 incorrect attempts and will remain locked until reset by one of the IT Service Desks or Libraries.**

**5.2.4. Your password must contain characters from the following:**

**5.2.4.1. upper case letters;**

**5.2.4.2. lower case letters;**

**5.2.4.3. numbers;**

**5.2.5. Further advice and guidance on selecting and maintaining your password can be found at https://en.support.wordpress.com/selecting-a-strong-password/**

6. *Offensive and other inappropriate material*

**6.1. You may not use the ICT Systems if the purpose or effect of such use is the downloading, viewing, listening to, posting, or circulation (whether over the Internet or otherwise) of information, e-mail messages, images, audio files or other data which are or which ICMP may reasonably consider to be offensive or inappropriate. This will include material which is or could be perceived as being:**

6.1.1. obscene or pornographic; or
6.1.2. racist, sexist or discriminatory or offensive in any other way (including, but not limited to, on grounds of disability, sexual orientation, age, or religion); or
6.1.3. politically extreme; or
6.1.4. defamatory; or
6.1.5. untrue, abusive or malicious; or
6.1.6. bullying or harassing; or
6.1.7. an infringement of the rights of any other person anywhere in the world; or
6.1.8. otherwise objectionable.

6.2. ICMP has a duty under the Counter-Terrorism and Security Act (2015), to prevent people being drawn into terrorism. To meet this duty ICMP's systems must not be used to create, access, transmit or download inappropriate materials as defined under the Prevent legislation. ICMP reserves the right to monitor, alert and report attempted access to, or dissemination of, such inappropriate material.

6.3. The definition of extremist material will be governed by Home Office definitions within the Prevent Guidance (2015).

6.4. The question of what constitutes offensive material is not one for the sender to determine - it is the effect on the recipient which is important. You should not therefore pass on any material which even risks causing offence to any recipient. For this reason, the circulation of e-mails and other materials containing strong language or offensive jokes is not permitted.

6.5. You must report to the IT Service Desk (who will treat this concern with confidentiality and refer the matter to an appropriate Senior Manager) any person you know or reasonably suspect to be acting in breach of this section of this policy and take immediate steps to prevent continued access to, or distribution of material from sites, or the sending of e-mails containing offensive or inappropriate material as described in paragraph 6.1.

6.6. If you feel that you are being harassed or offended in any way by the use of the facilities by any other student or member of staff (or even by people outside ICMP), whether or not such harassment or offence is intentional, you should report the situation to IT Services.

6.7. ICMP reserves the right to monitor all incoming internet traffic by scanning ICMP's web cache for such material and where there is a systematic or deliberate pattern of misuse, this will lead to formal action under our student disciplinary procedures.

6.8. In the event that a user is found to have accessed or received such materials, his or her internet, e-mail and telephone usage and data may be examined in detail to ascertain whether usage is part of a systematic pattern of misuse. No disciplinary action may be taken if the misuse is not systematic, as we recognise that users may receive occasional unsolicited messages or access an internet site in error. However, the user must immediately notify IT Service Desk upon receipt of or upon accessing any such material.

6.9. In the rare event that visits to obscene or pornographic web sites are required for legitimate academic purposes, permission for such usage must be sought in advance and in writing from the Dean of Academic Studies and notified in advance and in writing Business Development Director. The receipt and/or distribution of such material including the circulation of it to another user or users may also be a criminal offence and ICMP reserves the right to report any such incidents to the Police.

6.10. ICMP reserves the right to prevent access to materials it feels are inappropriate and also where ICMP is required to do so by Law, Policy or Statutory duty.

7. *Acceptable Use of e-mails and the internet*

**7.1. Do not download software, programs, music or other content (even if free) from the web onto the IT Systems. This prohibition extends to screen-savers and games.**

**7.2. You are reminded that e-mails are a form of written communication which is permanent and which may be read by any member of the public. You should therefore always consider whether it is appropriate to use e-mails for the particular communication envisaged. Please note that we may be required to disclose e-mail messages in legal proceedings relating to their subject matter and that the deletion of a message or file may not fully eliminate it from the IT Systems.**

**7.3. If it is necessary to send sensitive or confidential information by email, then care should be taken to provide a reasonable level of protection. You should be as careful about the content of e-mails as you would be with letters. Consider in every case whether the content of an e-mail would reflect well on ICMP and, in particular, you should make sure that:**

**7.3.1. all contents are accurate and appropriate for dissemination by e-mail;**

**7.3.2. disparaging or unduly critical comments are avoided;**

**7.4. The language of any e-mails you send should be in accordance with the standards of any other written communications and at all times the language used should be appropriate to formal business communications. You should under no circumstances use e-mails to spread gossip or similar information and the prudent test would be for you to write in e-mail form only such matters (and in such language) as would be considered suitable for a letter.**

**7.5. E-mail can sometimes be used as a medium for bullying and intimidating other people. This will not be tolerated. If you are unhappy about something please discuss the matter with your programme leader or academic manager.**

**7.6. If you generate or forward e-mails to others, you must be very clear as to the intended recipient. The inadvertent dispatch of material to a collective user group, for example, is no different from sending it individually to all those within that group.**

**7.7. Students must not accept or open any file received as an e-mail attachment if you are in any doubt as to its source, as you may spread a virus. If in doubt, contact the IT Service desk.**

8. *Copyright*

**8.1. Use of the IT Systems to copy or transmit any documents, software or other information protected by copyright is prohibited unless the permission of the copyright owner has been obtained. Remember that copyright extends to music and images as well as text. In particular, before copying any material from the Internet read the copyright notice on the site and be sure to comply with it. Take care even where the website says you may freely copy any material made available on it, because sometimes copyright or other rights in such material does not in fact belong to the owner of the website.**

9. *Security and Safeguarding the Network*

**9.1. You are responsible for the security of your laptop or computer terminal and must not allow your equipment to be used by any unauthorised person.**

**9.2. If you have cause to be away from your work station for any period and wish to avoid any risk of abuse of your equipment, you should log out or lock your equipment while absent. Otherwise we will be entitled to assume in the first instance that any material coming from or via your equipment was generated or passed on by you.**

*10. Monitoring and Processing of Data on IT Systems*

**10.1. Subject to the qualifications set out in this paragraph 6 we will treat all messages sent, received or stored using the ICT Systems as e-mails which relate to the operation, business or academic activities of ICMP and neither staff nor students should have any expectation of privacy in any such messages.**

**10.2. We reserve the right to access, review, copy, process, delete or otherwise process any messages sent, received or stored on the ICT Systems and to disclose any such e-mail messages (or information contained in them) to any person outside ICMP where this is necessary for any purpose in connection with your study in the following circumstances:**

**10.2.1. to detect the unauthorised use of the ICT Systems;**

**10.2.2. to protect the ICT Systems against viruses or hackers;**

**10.2.3. to find lost messages or retrieve messages due to computer failure;**

**10.2.4. to assist in the investigations of wrongful acts (including further investigation where a routine audit has revealed a breach of this policy or the breach of any relevant regulatory or self-regulatory practices or procedures);**

**10.2.5. to combat or investigate fraud or corruption;**

**10.2.6. to prevent or detect crime; or**

**10.2.7. to comply with any legal obligation.**

**10.2.8. to prevent the receipt of unsolicited communications that do not relate to the operation, business or academic activities of ICMP.**

**10.3. We will take all reasonable steps to avoid opening or otherwise viewing the contents of e-mails which are marked "personal" in the subject heading unless we believe that such action is required in the circumstances set out in paragraph 2. E-mails marked "personal" will be subject to traffic monitoring and automated interception to check for viruses in the same way as all other e-mails sent or received using the ICT Systems.**

**10.4. We also reserve the right to monitor students' access to the Internet for any purpose in connection with engagement or study with ICMP and in the following circumstances:**

**10.4.1. to prevent or detect crime;**

**10.4.2. to detect the unauthorised use of the Internet;**

**10.4.3. to protect the IT Systems against viruses or hackers; or**

**10.4.4. to combat or investigate fraud or corruption.**

**10.5. Where possible monitoring of e-mail and Internet traffic will be limited to audits and monitoring traffic data unless routine monitoring or auditing justifies more detailed monitoring. However, we reserve the right to restrict access to individual or groups of a website should it be deemed appropriate to do so. Where possible automated monitoring will be used.**

**10.6. Information generated by monitoring Internet access and e-mail traffic will not normally be retained by us for more than one year. You are warned however that copies of all e-mails sent and received using the ICT Systems can normally be retrieved after a significantly longer period, whether or not they are marked "personal".**

*11. Data protection*

**11.1. You should also refer to our Data Protection Manual which is available on our website and VLE. You are reminded of the need to comply with the provisions of the Data Protection Act 1998, in particular with regard to the need to ensure the security**

**and confidentiality of personal data (that is any information from which a living individual can be identified).**

*12. Leavers*

**12.1. On leaving ICMP students' e-mail accounts will be disabled and IT Services will be notified of leavers on a monthly basis.**

**12.2. In the event that it is deemed necessary to disable a student's e-mail account immediately, we reserve the right to action this without prior notice.**

**12.3. All leavers should therefore make all efforts to remove all documents before the account is closed. ICMP cannot be held accountable for the loss of documents.**

*13. Discipline*

**13.1. Failure to adhere to this policy may result in disciplinary action, ranging from revocation of network access to withdrawal from your programme of study.**

**13.2. Breaches of this policy which have serious or potentially serious adverse consequences for the operation, business or academic activities or reputation of ICMP or the security and integrity of the IT Systems and any breaches of section 6 of this policy may render a student in breach and liable to expulsion.**

*14. Equality Impact Assessment*

**14.1. The policy has been designed to ensure that all sections of our community can engage fully with our IT provision and have equal access to it.**