ICMP

The Institute of Contemporary Music Performance

Acceptable Use of IT Policy

Version number	Date approved (including committee)	Reason for production/revision	Author	Proposed next review date
V2.1	Sept 2023 IGG	Periodic review	IT Manager	Q1 2025-26
V2	Sept 2021 ExCo	Alignment with the Information Governance Framework	IT Manager	Biannually and as required
V1.5	July 2019	Annual review	IT Manager	Biannually and as required

Related policies

- Data Protection Policy
- Freedom of Information Policy
- Employee Records Data Protection Policy
- Records Management Policy
- Data Security Policy
- E-mail Use Policy
- Bring Your Own Device Policy
- Business Continuity Policy
- Staff Disciplinary Policy
- Student Disciplinary Policy
- Equality & Diversity Policy
- Safeguarding Policy
- Access and Monitoring Policy
- Clean Desk and Screen Policy
- Learning Analytics Policy

External Reference

- Counter-Terrorism and Security Act (2015)
- Prevent Guidance 2015 (updated 2021).

1. Definitions

1.1. "**ICT Systems"** includes central services as provided by ICMP such as e-mail, networks, internet access, computers, computing equipment and mobile devices, personally owned computers and devices when connected to, or accessed from or via

ICMP facilities,

- use of remote networks and services, when accessed from or via ICMP ICT Systems;
- 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, staff, workers, honorary title holders, visiting academics 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 'physical' or 'paper' files.

2. Purpose and scope

2.1. This policy sets out the standards which apply to all users in their use of ICMP's ICT Systems including personal devices.

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:

- claims brought against ICMP because the reputation of other individuals or organisations has been damaged;
- unauthorised disclosure of information, which is confidential to ICMP or its staff and/or students;
- 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);
- harassment and discrimination claims being brought against ICMP (caused by offensive or other inappropriate material);
- entering into contracts on behalf of ICMP by mistake;
- inadvertent breach of contract by ICMP;
- the introduction of viruses and/or malware 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. Please refer to the relevant staff or student disciplinary procedures for further details.

2.5. This policy applies to all users in whatever location they are working whether or not on our premises.

2.6. This policy considers 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. Use of Cloud Based and Portable Storage.

3.1. USB (external) storage devices should not be used by staff to store any confidential or personal information under any circumstances with the exception only of encrypted and password protected devices approved for this purpose.

3.2. ICMP utilises Microsoft 365 cloud storage solutions.

3.3. No ICMP data should be stored (particularly confidential or personal information) on any device outside of the ICMP with the exception of devices meeting the security requirements herein.

3.4. Use of any external or remote storage systems must conform to ICMP data storage policies as outlined in this document. This includes;

- use of appropriate passwords and security mechanisms;
- that all instances of use are communicated and approved by line managers;
- that all data processed on these devices is done so in line with the ICMP Data Protection Policy.

4. Disabled Students and Staff

4.1. The IT systems in use are regularly reviewed to ensure they are inclusive. Please refer to our Inclusive Practice Action Plan or contact ICMP 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 staff and Student Disciplinary Procedures as appropriate.

5.2. All users must register a secondary device to enable their Microsoft 365 account. This device is used for secondary authentication and password resets.

5.3. Your password must conform to the following.

- Passwords must be at least 8 characters long
- Passwords cannot contain your name or user name
- Accounts are locked after a set number of failed attempts (6). They are reset via the secondary device for 365 accounts or by the ICMP Data Team for ICMP accounts.
- Your password must contain characters from the following:
    - upper case letters;
    - lower case letters;
    - numbers;
- Further advice and guidance on selecting and maintaining your password can be found at https://en.support.wordpress.com/selecting-a-strong- password /

6. Acceptable Use of ICT Systems

6.1. As a general rule ICMP ICT Systems should be used solely for ICMP academic and business purposes. Limited use of the ICT Systems for personal reasons is acceptable provided that:

- the usage is minimal and, if you are a staff member, takes place wherever possible outside core operational hours (i.e. before or after work or during any permitted lunch break);
- the usage does not affect or interfere with the operation, business or academic activities of ICMP in any way;
- you do not enter into any contracts or commitments in the name of or on behalf of ICMP;
- the usage does not commit ICMP to any costs;
- the usage conforms to the guidelines set out in this policy.

6.2. Never send e-mails or access the Internet under a name other than your own..

7. Offensive and other inappropriate material

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

- obscene or pornographic; or

- 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
- politically extreme; or
- defamatory; or
- untrue, abusive or malicious; or
- bullying or harassing; or
- an infringement of the rights of any other person anywhere in the world; or
- otherwise objectionable.

7.2. 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.

7.3. The definition of extremist material will be governed by Home Office definitions within the Prevent Guidance 2015 (updated 2021)..

7.4. 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.

7.5. You must report to the IT Service Desk (who will treat this concern with sensitivity) 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 7.1.

7.6. 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.

7.7. 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 staff or student disciplinary procedures.

7.8. In the event that a user is found to have accessed or received such materials, their ICT usage 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.

7.9. 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 Principal.

7.10. 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.

7.11. 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.

8. Acceptable Use of the internet

8.1. Do not download software, programs, music or other content (even if free) from the web onto the IT Systems unless such download is necessary in the proper performance of your duties if you are staff member and even then, do not do so without the prior written/e-mail permission of the IT Services Team. This prohibition extends to screen-savers and games.

9. Websites

9.1. We have a website on the Internet, currently situated at icmp.ac.uk. Your use of the website is subject to the terms of this policy and to any terms of use posted from time to time on the website.

9.2. If you are involved in updating or maintaining our website including any links contained on the web site, you should ensure that

- any third parties, including designers or other self-employed consultants commissioned to work on the website have signed a written contract with ICMP (in a form approved by ICMP) in advance of commencing work to ensure that ICMP obtains ownership of the relevant copyright and other rights in their work; and

- Information placed on our website is accurate and complies with all legal requirements and has been approved in accordance with our internal procedures.

9.3. If you find anything incorrect or out of date on our website, you should report it immediately to the marketing team and/or the person(s) responsible for the relevant part of the website so that steps may be taken to correct the website as soon as possible.

9.4. We own or are licensed to use all copyright, other intellectual property rights in and pertaining to the website, its design and content, and all technical infrastructure relating

to it. The trademarks and logos displayed on the website are ICMP's registered and unregistered trademarks or those of others. You should not use any of the trademarks or other material on the website other than in accordance with this policy and any terms of use posted from time to time on the website.

10. Copyright

10.1. 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.

11. Security and Safeguarding the Network

11.1. 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.

11.2. You must ensure any computer you use to access our IT Systems is protected with anti-virus software which is kept up to date.

This is provided automatically for ICMP computers however BYOD users should refer to the advice providedthe IT Service Desk.

11.3. If you have cause to be away from your work station for any period you should log out or lock your equipment, 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. See ICMP's Clean Desk and Screen Policy for further guidance.

12. Software Use and Installation Restrictions

12.1. Software is subject to copyright and licensing restrictions. Software provided by ICMP should only be used by members of ICMP for academic, research and administrative purposes, and you should not copy or distribute it to others unless authorised to do so.

12.2. Do not install software onto our IT systems without obtaining permission from the IT Department. You should not knowingly install software onto any of our IT systems (desktop systems and servers), without obtaining permission from the IT Department.

13. Data protection

13.1. You should also refer to our Data Protection polices and our wider Infromation Governance guidance which are available on My.ICMP. You are reminded of the need to comply with the provisions of the Data Protection Act 2018, 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).

14. Leavers

14.1. On leaving ICMP Staff user's e-mail accounts revert to ownership by the company.

14.2. Staff are expected to remove any personal information from the e-mail account.

14.3. Staff leavers accounts will usually be deleted after a short period of mail forwarding and auto-reply notifying senders of the departure. The account will only retained where company data is held within and required for company business.

14.4. On leaving ICMP Student user's e-mail accounts will be disabled or downgraded to 'e-mail only' status for alumni. Leavers will be provided with the date of this action.

14.5. In the event that it is deemed necessary to disable a user's e-mail account immediately, ICMP reserve the right to action this without prior notice.

14.6. 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.

15. Acceptable use of Telephones

15.1. As with e-mail, a reasonable amount of personal use by staff is permitted without charge, provided that such use is limited to emergency and occasional local calls of short duration.

15.2. Staff may not make long distance calls or local calls of longer duration without line management consent. Such calls will be charged for by ICMP and please liaise with your manager to ensure the call duration and cost are recorded so the necessary deduction can be made directly from your salary.

16. Discipline

16.1. Failure to adhere to this policy may result in disciplinary action. Please see the relevant staff and student disciplinary procedures for more information.

16.2. 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 7 of this policy may render a student or staff member in breach eligible for gross misconduct or withdrawal from programme.

17. Interpretation

17.1. This policy cannot cover every eventuality, particularly as the technology and its application is changing so rapidly. You are required to consider the purpose and objectives of this policy and to acknowledge that there are some uses of the Internet, e-mail facilities and related technology which, while not expressly forbidden by this policy, may still be regarded as inappropriate.

17.2. This policy will be reviewed and updated on a regular basis.

18. Equality Impact Assessment

18.1. 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.