Access and Monitoring Policy

Version number	Date approved (including committee)	Reason for production/revision	Author	Proposed next review date
V1.0	Sept 2021 ExCo	Produced to align with the Information Governance Framework	IT Manager	Biennially and as required

Related policies
Data Protection Policy Freedom of Information Policy Employee Records Data Protection Policy Records Management Policy Data Security Policy Email Use Policy Acceptable Us of IT Policy Bring Your Own Device Policy Business Continuity Policy Staff Disciplinary Policy Student Disciplinary Policy Equality & Diversity Policy Safeguarding Policy
External Reference
General Data Protection Regulation (GDPR), UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation (PECR)

ICMP

The Institute
of Contemporary
Music Performance

1. Purpose

1.1. ICMP has a duty to inform its users on the extent to which monitoring and interception of information on computer systems and networks is carried out.

1.2. The IT team as the responsible agency for IT Systems and services at ICMP, carries out monitoring of a variety of information.

1.3. Monitoring takes place for operational purposes, such as:

1.3.1. to maintain and enforce network security

1.3.2. To maintain and monitor the integrity of IT systems

1.3.3. To protect against viruses and SPAM

1.3.4. To check for misuse of resources

1.3.5. To gather usage statistics

1.3.6. Network traffic for usage controls

1.3.7. Telephone usage for charging purposes

1.3.8. Data audit trails for systems where appropriate

1.4. Monitoring may take place for the prevention or detection of crime.

1.5. All monitoring logs will be kept for a minimum period of three months.

1.6. The Executive Committee reserves the right to examine any machine connected to ICMP's network that is affecting IT systems or suspected to be contravening the conditions of use.

1.7. Authorisation for monitoring processes must include at least 2 members of the Executive Committee, including at least 1 company director.

1.8. ICMP observes that the legislation sanctions the interception and monitoring of communications, placing limits on the powers of the organisation and the protection for the rights of individuals.

1.9. IT staff will not routinely monitor or inspect

1.9.1. the contents of electronic mail folders

1.9.2. the contents of any personal file store

1.9.3. telephone calls except in the case of call recording for training purposes

1.10. However inspection may take place by a Company Director, or designated officer if

1.10.1. A routine access to business communications is required when staff users are on holiday or sick

1.10.2. An alleged misuse is bought to the attention of a Company Director

1.10.3. A request is made by police as part of an enquiry.

1.11. Information gathered into logs can be found in section 4 of this document.

2. Scope

2.1. This policy applies to all users of ICMP's IT services and therefore includes all staff, students, contractors, representatives or guests who utilise ICMP's IT systems

3. Guidelines for inspecting user material

3.1. In the following user material is defined as all user owned files and electronic mail folders. Authorization to inspect user material will be given by a Company Director.

3.2. Authorised users of IT systems should be aware that personal communications, as well as communication relating to ICMP business made via ICMP IT systems may be monitored or intercepted whilst carrying out inspections.

3.3. All staff given privileged access to systems and networks must respect the privacy and security of the user material.

3.4. Staff responsible for the management operation or maintenance of systems and networks have the right to access user material and monitor network traffic, but only if necessary to fulfil their role.

3.5. Authorization and examination should not be carried out by the same person.

3.6. If examination proceeds in circumstances where it is not possible to get the user's permission in advance, then the user should be informed after the event.

3.7. A record should be kept of any such examination. Such a record should be available for inspection.

4. Monitoring and Processing of Data on IT Systems

4.1. Please see the Email Policy for details of email monitoring

4.2. Information gathered by IT Services as part of the Systems, Network and Telephony Monitoring Process includes:

4.2.1. Account Information. Maintenance of computer accounts is automated in the case of students, based on data taken from the student records system. In the case of staff, a manual system is applied which records similar data.

4.2.2. Access Logs. Monitoring of the following is logged into separate places and can only be related to individuals by bring the information together. The following list are monitored in accordance with this policy

4.2.2.1. Logon to the network

4.2.2.2. Logon to ICMP servers

4.2.2.3. Access to network drives from PCs

4.2.2.4. Access to Exchange based mail servers including IMAP and SMTP

4.2.2.5. Electronic mail messages posted or delivered on ICMP servers

4.2.2.6. Web pages accessed on ICMP servers

4.2.2.7. Web pages accessed on the Internet by ICMP clients

4.2.2.8. Access to file transfer (ftp) servers

4.2.2.9. IP Traffic Monitoring

4.2.2.10. Telephone System