ICMP

The Institute
of Contemporary
Music Performance

Bring Your Own Device Policy

<table>
<tr><th>Version number</th><th>Date approved (including committee)</th><th>Reason for production/revision</th><th>Author</th><th>Proposed next review date</th></tr>
<tr><td>V1.0</td><td>Sept 2021
ExCo</td><td>Produced to align with the Information Governance Framework</td><td>IT Manager</td><td>Biennially and as required</td></tr>
<tr><td colspan="5"><b>Related policies</b></td></tr>
<tr><td colspan="5">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
Business Continuity Policy
Staff Disciplinary Policy
Student Disciplinary Policy
Equality & Diversity Policy
Safeguarding Policy</td></tr>
<tr><td colspan="5"><b>External Reference</b></td></tr>
<tr><td colspan="5">General Data Protection Regulation (GDPR), UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation (PECR)</td></tr>
</table>

1. Purpose

1.1. ICMP is committed to preserving the confidentiality, integrity and availability of its data. The use of their own devices by employees for work purposes can be beneficial to ICMP but it also introduces new risks.

1.2. ICMP does not have any control on the security mechanisms implemented on an employee's personal device. If your personal device was lost or stolen there would be a risk that any ICMP information stored on it could be accessed and exploited by unauthorised individuals.

1.3. You are accountable for the security of the information whilst it is on your device. Should the ICMP data held on your personal device be lost, stolen or the data is compromised, this will constitute a breach of the Data Protection Act 2018 and the loss will be investigated. As part of this investigation, you will be required to explain the steps taken to ensure the security of the data and the device.

1.4. ICMP reserves the right to refuse to allow access to particular devices or software where it considers that there is a security risk to its systems and infrastructure.

1.5. Failure to comply with this policy may constitute grounds for action under ICMP's disciplinary procedure

2. Scope

2.1. 2.1 This guidance applies to ICMP employees who use their personal device to process ICMP data. This is commonly known as "Bring Your Own Device" or BYOD.

2.2. For the purposes of this document personal devices include but are not limited to home desktop PCs, tablets (iPads etc), smartphones, laptops, video and audio recording equipment.

2.3. Staff should note that if conducting ICMP business then the Acceptable Use of IT policy must be adhered to regardless of the platform that the work is being undertaken upon.

3. Policy

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

3.1.1. 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;

3.1.2. invoke the relevant security features

3.1.3. maintain the device themselves ensuring it is regularly patched and upgraded.

3.1.4. enable encryption on your device. If it is not possible to encrypt your device, you must not store personal data on it. You must also not store any data that if it were compromised could have an adverse effect on the reputation of ICMP or the ability of ICMP to function.

3.1.5. only copy data to your mobile device if there is a legitimate need to do so and only if there is no alternative. Once it is no longer necessary you must completely remove the data from your device including any email attachments containing data.

3.1.6. back up all data to ICMP’s 365 services to ensure that a unique copy is not stored on your device.

3.1.7. set your device to lock automatically after a small period of inactivity. The period of inactivity set should be no more than 2 minutes.

3.1.8. install and configure tracking services such as “Find my Phone” or “Where’s my Droid”.

3.1.9. configure your device so that in the event of it being lost or stolen it is possible to remote wipe its contents. If that is not possible you should set it to auto wipe the contents if the wrong PIN/password is entered ten times.

3.1.10. ensure that your device’s software is up to date and that it has the latest security patches installed.

3.1.11. Install if it is available for your device anti-virus software and ensure that it is kept up to date.

3.1.12. Ensure that other members of your household who may use your device cannot access ICMP data.

3.1.13. completely remove all ICMP information from your device once you cease to work for ICMP. This should be done by returning your device to manufacturer’s settings.

3.1.14. completely remove all ICMP information from your device by returning it to the manufacturer’s settings before you sell, exchange or dispose of i

3.1.15. configure your device to not to automatically connect to available wireless access points. You must use your judgement about the security risk of connecting to a wireless network before doing so. You may have to account for your decision at a later date.

3.1.16. exercise caution when downloading apps to your device. Malicious apps have been located in both the Google Play store and the Apple iTunes App store.

3.1.17. report it immediately to your line manager if your device is lost or stolen. You should also immediately change the passwords to all of ICMP’s services accessed from the device.

3.1.18. abide by the contents of the Acceptable Use of IT Policy and other appropriate ICMP Information Security policies and guidance when using your personal device for work purposes.

3.1.19. contact the IT team before taking your personal device to an external organisation for repair if you use it to process ICMP personal or confidential data.

4. Monitoring

4.1. ICMP will not monitor the content of your personal device but reserves the right to prevent access to ICMP systems by any device that is considered a risk. ICMP also reserves the right to monitor and log data transferred between your device and its systems.

4.2. In exceptional circumstance it may be necessary for ICMP to access ICMP data that is stored on your personal device. Every effort will be made to ensure that your personal data on the device will not be accessed.