Mobile Device Management Policy

Policy name: Mobile Device Management Policy
Governance Committee Approved: 13/03/2023

Approved by Trinity Academic Council: 15/11/2023
Approved by RIAM Governing Body:13/04/2023

1. Context

The Royal Irish Academy of Music, hereinafter referred to as RIAM or the Academy, recognises the importance of staff usage of mobile phones, smart devices (such as iPads or Tablets), laptops, MAC Books and other portable equipment (hereinafter referred to as 'Mobile Devices') in carrying out their administrative and teaching duties.

This policy is designed to clarify the correct and acceptable use of and management of mobile devices business use.

2. Purpose

The RIAM is committed to the correct and proper use of Mobile Devices in support of its administrative and teaching functions. The inappropriate use of such devices could expose the RIAM to risks including, theft and / or disclosure of information, disruption of services, fraud or litigation. The purpose of this policy is to define acceptable, safe and secure standards for the use and management of Mobile Devices within RIAM.

3. Scope

This policy applies to all mobile phones, iPads, Tablets, MAC Books, laptops, notebooks and other physical ICT equipment, owned or leased by RIAM and users and holders of all such devices. All mobile devices provided to staff by RIAM for the performance of their duties remain the property of RIAM at all times.

4. Policy & Procedures

4.1 Assignment and Allocation of Mobile Phones to Staff

The allocation of a mobile phone must be approved by the relevant manager and in conjunction with ICT/HR, in circumstances where there is an adequate need or benefit to the RIAM. These circumstances include:

- The requirement for an employee to undertake frequent out-of-office duties, including meetings or travel.
- When an employee is on-call or stand-by (a phone may be given on a shared basis for use by a designated office).
- In relation to the function or role, eg, security, customer facing or contact function.
- For greater efficiency and enhanced client service.
- The employee has been identified as a key member of staff who needs to be contactable at all times.
- The employee's duties are such that a mobile phone is required for health and safety reasons (for example lone working).

- At the discretion of the Director or Finance Officer.

Once a decision has been made about the allocation of a mobile phone the relevant manager should write to the Finance Officer and ICT Manager by email, informing them and requesting budgetary approval.

Please note that employees who are not allocated an RIAM mobile phone may be asked to download software to a personal device to allow them to make or receive phone calls on behalf of RIAM at no cost or risk to the employee.

4.2 Assignment and Allocation of Smart Devices (other than mobile phones) and other portable ICT equipment such as printers, monitors, keyboards, mice, docking stations etc.

The allocation of a device must be approved by the relevant manager and in conjunction with ICT/HR, in circumstances where there is an adequate need or benefit to the RIAM. These circumstances include:

- The requirement for remote working on behalf of RIAM on a site other than the main office.
- In relation to a function of the role such as teaching.
- The employee's duties are such that the equipment is required for health and safety reasons.
- At the discretion of the ICT Manager, Director or Finance Officer.

Please note that employees who are not allocated an RIAM Smart Device may be asked to download software to a personal device to allow them to make or receive phone calls on behalf of RIAM at no cost or risk to the employee.

4.3 Procurement of Mobile Devices.

All mobile devices must be purchased in line with the RIAM Procurement Policy. Only devices that have been procured by RIAM and are owned by RIAM will be allowed connection to the RIAM network. All devices remain the property of RIAM.

If an employee has been approved for receipt of an upgraded device, all previously held devices must be returned to the ICT manager for use by other staff or recycling as appropriate.

4.4 Responsible Use and Security

The inappropriate use of mobile devices could lead to theft and/or disclosure of private or confidential organisational information. The devices may only be used by the assigned employee or department and must ensure that usage is lawful and ethical. Mobile devices represent a significant risk to information security as they can easily become a conduit for unauthorised access to RIAM's data and ICT infrastructure, which could lead ultimately to data leakage and system infection.

- Employees who are allocated a device are reminded that the equipment is the organisation's property and ultimate liability for its misuse rests with the user and the organisation.

- Employees should not access, store or distribute any offensive or inappropriate (e.g. defamatory or racist) material on the device (*see organisation's data protection and bullying and harassment policy for further information*).
- The number of calls and texts and the length of calls made on mobile phones should be limited to those necessary for effective business use.
- Reasonable care must be taken to prevent accidental damage, loss or theft of equipment. In the event of the theft or loss of equipment, the user must immediately contact the ICT Manager. RIAM equipment is not to be left in vehicles while unattended.
- Employees are requested to personalise and activate the messaging service of their mobile phone. Ensure that you have recorded your name plus the organisation name so that the caller knows he/she has reached the correct number.
- Storage and protection settings such as PIN numbers and secure passwords are applied to mobile phones, tablets, iPads, MAC Books and Laptops. Please ensure these facilities are used at all times to minimise security risks as discussed in this policy.
- With the exception of those devices managed by ICT, devices are not allowed to be connected directly to the internal business network
- Devices must be kept up to date with critical security patches provided by the manufacturer. It is the employee's responsibility to manage and download all available operating software updates.
- RIAM users must not load pirated software or illegal content onto their devices.
- Devices must not be connected to RIAM Networks and/or other devices which do not have up-to-date and enabled anti-virus/malware protection
- Users must ensure that they use RIAM devices at all times in a manner which is lawful, ethical and efficient. The RIAM may withdraw a device from any employee who it believes is not complying with this policy or who misuses a device in any manner.
- Users must make every reasonable effort to ensure that their RIAM device is secured at all times, kept charged and switched on during working hours
- Only software which has the correct and proper license and has been purchased and/or approved by the ICT Manager may be installed and used on an RIAM Device.
- RIAM Devices may only be used by an assigned RIAM employee and must not be used by any other RIAM employees or third parties without the prior authorisation of the ICT Manager.
- The RIAM reserves the right to monitor, capture and inspect any phone call information made on an RIAM mobile phone device or on an RIAM phone account, in order to:

  a) Investigate system problems;
  b) Investigate potential security violations;
  c) Maintain system security and integrity;
  d) Prevent and detect misuse;
  e) Review expenditure charged to a mobile phone device telephone account with a view to seeking reimbursement from RIAM employees in respect of all costs relating to the personal usage of their RIAM mobile phone device;
  f) Ensure compliance with RIAM policies, current legislation and applicable regulations.

  While the RIAM does not routinely monitor an individual user's device activity, it reserves the right to do so when a breach of its policies or illegal activity is suspected. This monitoring may include but is not limited to details of telephone calls made, messages and emails sent to and from the device, internet access and information stored on the device. The monitoring of an individual user's device activity must be authorised by the HR

Manager and the individual's line manager. The results of all monitoring will be stored securely and will only be shared with those authorised to have access to such information.

- Users must take all reasonable steps to prevent damage or loss to their device. This includes not leaving it in view in an unattended vehicle and storing it securely when not in use. The user may be held responsible for any loss or damage to the device, if it is found that reasonable precautions were not taken.

- Incidents where a lost or stolen RIAM device contained confidential or personal information must be reported and managed in accordance with the RIAM Data Protection Management Policy

4.5 Use of Mobile Phones while Driving

Extreme care should be exercised when using mobile phones in cars. Under Section 3 of the Road Traffic Act 2006, mobile phones can only be used when connected to a hands free unit. Employees who are required to travel frequently for work and who are allocated a mobile phone will be provided with a hands free unit for their car, if requested. However, it is organisation's policy that employees do not answer or make calls whilst driving.

It is an offence to drive a vehicle while holding a mobile phone. An offence is committed by holding a mobile phone while driving and matters such as whether or not the phone was being used or switched on at the time are not relevant. Any employee who commits an offence under this legislation will be personally responsible and liable for any costs incurred.

4.6 Personal use of Devices

RIAM devices are to be used primarily for RIAM work-related purposes. Occasional and limited personal use may be permitted.

5. Unacceptable Use

RIAM mobile devices and ICT equipment may not be used:

- For excessive personal use;
- For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
- For political activities; such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
- To knowingly misrepresent the RIAM;
- To transmit confidential or personal data outside the RIAM unless the data has been encrypted;
- To send text messages or emails which contain any confidential and/or personal information regarding the RIAM, it's staff or students;
- To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
- To view, create, download, host or transmit (other than for properly authorised and lawful purposes) pornographic, offensive or obscene material (i.e. information, images, video clips, audio recordings etc), which could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs;
- To retrieve, create, host or transmit any material which is designed to cause annoyance, inconvenience or needless anxiety to others;

- To retrieve, create, host or transmit material which is defamatory;
- For any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
- For any activity that would compromise the privacy of others;
- For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the RIAM or others;
- For any activity that would intentionally waste the RIAM's resources (e.g. employee time and IT resources);
- For any activity that would intentionally compromise the security of the RIAM's IT resources, including the confidentiality and integrity of data and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
- For the installation and use of software or hardware tools which could be used to probe, and / or break the RIAM IT security controls;
- For the installation and use of software or hardware tools which could be used for the unauthorised monitoring of electronic communications within the RIAM or elsewhere;
- For creating or transmitting "junk" or "spam" emails. This includes unsolicited commercial emails, chain-letters or advertisements;
- For any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

5. Employee's leaving

Employees must return all RIAM ICT Devices including mobile phones, iPads, tablets, laptops, MacBook, notebooks and other ICT equipment to the ICT Manager before they leave the employment of RIAM.

If an employee who has been engaged on a in one area/faculty of RIAM and is then moving to another area/faculty and no longer requires the mobile device for the execution of their duties, they must return the mobile device to the ICT Manager immediately.

In the instance where an employee is on leave, or not actively working for RIAM for a prolonged period of time (60 days or more), for foreseen reasons (e.g., on a career break or otherwise, the employee should not continue to use RIAM provided devices, unless with agreement of line manager and HR. This includes, but is not limited to, career breaks, long term sick leave, carers leave and other forms of protected leave.

The employee may be asked to return the mobile device(s) for the temporary period of leave, or may be asked to facilitate routine software updates during that period where the device(s) remain in their care.

Employees may request the continued use of devices during their time of leave, at the discretion of their line manager in conjunction with the ICT manager.

All devices must be returned with open access or relevant login or PIN

6. Records

The ICT Manager should record:

a) Assignment of device (Employee name, location, contact details, position and email address); b) Mobile phone device telephone number or serial number of other devices; c) Date the mobile device was issued; c) Dates and details of any upgrades or replacements; d) Dates and details of any associated equipment (e.g. car kit, battery charger, docking station etc.) supplied with the mobile device; e) Details of any restrictions applied; f) Review date.

b) All records will be held in accordance with the RIAM GDPR policy and records retention policy.

7. Responsibility

The responsibility for the correct use of these devices rests with all staff, who use or have involvement with the systems. Both the RIAM ICT user community and ICT services have responsibilities to ensure compliance with this policy.

Staff who have use of any RIAM device should ensure the device is maintained in good order, adhere to proper operating instructions, take appropriate security measures to avoid theft and report lost, stolen or damaged equipment to their line manager or the ICT Manager.

The RIAM Senior Management team has overall responsibility for the Mobile Device Management Policy. Appropriate procedures must be in place together with management, monitoring and review processes to ensure that policies are implemented, adhered to and kept up-to-date.

The ICT Steering Committee oversees the ICT infrastructure, database systems and assets, makes recommendations to Senior Management, reports on ICT security matters and ensures that policies are implemented in order to avoid breaches of legal, statutory, regulatory, contract or privacy obligations.

The ICT Manager plays a key role in the implementation of the Mobile Device Management Policy and has responsibility for monitoring the RIAM network infrastructure, including all hardware and communication links, reporting any audit issues that may be identified in relation to these items, and providing advice and assistance to end users.

8. Legislation and Regulation

Copyright and Related Acts 2000, 2004 and 2007

Data protection Act 2018

Child Trafficking and Pornography Act 1998.

Child Trafficking and Pornography Act 2004

Criminal Damages Act 1991

Defamation Act 2009

Employment Equality Act 1998

Equal Status Act 2000

Equality Act 2004

Prohibition of Incitement to Hatred Act 1989

Qualifications and Quality Assurance (Education and Training) Act 2012

Standards and Guidelines for Quality Assurance in European Higher Education Area (2005)

GDPR 2018

National Framework of Qualifications (NFQ).

Records Management and Retention Policy

Data Protection Policy

9. Related Documents

Staff Disciplinary Policy

Staff Grievance and Mediation Policy

Staff Code of Conduct

E-Communications Policy

ICT Policy

Social Media Policy

Dignity and Respect Policy

Flexible and Remote Working Policy

Health and Safety Statement

Career Break Policy

10. Document Control

Approved by RIAM Governing body: 13/04/2023
Approved by Trinity Academic Council: 15/11/2023
Next review: Academic year 2026/2027

11. Review

This policy will be reviewed on a three year cycle, or as required to take into account changes in the law and the experience of the policy in practice.