# RMF Information & Communication Technology (ICT) Usage Policy

**First version date: August 2020**

**Latest version date: February 2021**

**Next review date: February 2022**

# RMF Information & Communications Technology (ICT) Usage Policy

## A) INTRODUCTION

### 1) Purpose

a) This policy is designed to clarify and provide guidance on the appropriate use of Russell Martin Foundation's Information & Communications Technology equipment and systems in order to protect the privacy and integrity of data, and to mitigate the risks of security threats to its network.
b) Russell Martin Foundation is referred to as 'RMF' and 'the foundation'.
c) Information & Communications Technology equipment and systems are referred to as 'ICT'.
d) The policy will hold the standards, laws and guidelines whilst the procedure will describe the tasks and actions required.
e) The aim of this policy is to be helpful, and to set guidelines on the use of ICT at work for the smooth and efficient running of RMF's activities and business.
f) If there is anything in this policy and usage rules that a User considers to be unworkable, or does not understand, they should notify their Line Manager.

### 2) Scope

a) This ICT Usage Policy applies to the following: all RMF staff, including all employees, volunteers and trustees (referred to as Users).
b) This policy document covers:

i. General Principles
ii. Use of ICT
iii. General Communication Principles
iv. Mobile Phone Use
v. Use of Internet and Social Networking Sites
vi. Online Viewing and TV
vii. Email
viii. Security
ix. Safeguarding and Remote Education During Coronavirus
x. Monitoring
xi. Misuse and Compliance
xii. Policy Review and Related RMF Policies

## B) POLICY

### 1) General Principles

a) It is RMF's approach that Users are encouraged to use ICT in relation to the RMF's activities and business. However, Users are required to follow the rules outlined in this policy.
b) Any breach of this policy could result in disciplinary action, up to and including dismissal.
c) Any User who is unsure about whether something they propose to do might breach this policy, should seek advice from their Line Manager.

### 2) Use of ICT

a) Users are encouraged to use communication technology, including email and the internet at work as a fast and reliable method of communication with significant advantages for business.
b) All communications made by Users reflect upon RMF, and are capable of creating a number of commercial, professional and legal problems for RMF.
c) This policy is intended to clarify what RMF expects from Users and their responsibilities when using RMF's information technology and communications facilities.
d) ICT facilities, equipment and systems include but are not limited to:

i. Telephones or radio communicators (mobile or fixed)
ii. Personal or portable computers
iii. Email
iv. Internet and intranet
v. Video conferencing facilities
vi. Printers, IT storage devices or other such associated ICT equipment and peripherals
vii. Any other communication device or network provided by RMF

e) Whilst the ICT equipment and systems provided by RMF are made available to Users for the purposes of the business, a certain amount of limited personal use is permitted provided such personal use is consistent with this ICT Usage Policy and the duties of the User.
f) All ICT equipment and systems are and remain the property of RMF and should always be treated with suitable care to avoid loss or damage to all or any part of it.
g) RMF laptops and storage devices must always be locked in a secure area when not in use and should never be left unattended and on display in vehicles.
h) Laptops should always be carried in their protective case.
i) RMF does not allow Users to bring software or hardware into the office without consent. Only authorised software is to be loaded on RMF machines or systems.

### 3) General Communication Principles

a) There are certain general principles that should be born in mind when using any type of communication, be it external or internal, including hard copy letters, memos and notices.
b) RMF expects all Users to:

i. Use communications equipment and facilities responsibly and professionally, and at all times in accordance with their duties, including RMF letterhead and stationery.
ii. Be mindful of what constitutes confidential or restricted information and to ensure that such information is never disseminated in the course of communications without express authority.
iii. Ensure that they do not bind themselves or RMF to any agreement without express authority to do so.
iv. Be mindful of the fact that any communications may be required to be relied upon in court, to the advantage or the detriment of the individual or the foundation, and conduct their use of communications systems and equipment accordingly
v. Avoid making remarks or comments on personal or social networking sites that may be deemed derogatory, regardless of whether they are made in or out of work.
vi. Ensure that they do not breach any copyright or other intellectual property rights when making communications.

## 4) Mobile Phone Use

a) RMF mobile phones should only be used, (other than in an emergency), for business related calls. Where personal phones are used for RMF business, this must be authorised by management.
b) Users should take care of any RMF mobile phone issued to them and ensure it is secure at all times. If the phone is lost or stolen, the User should notify management immediately so appropriate steps can be taken to disconnect it.
c) Personal mobile phones or other personal audio-visual systems should not be used to send or receive private calls or text messages or listen to music during working hours except in an emergency or by agreement with the User's manager.
d) Users should not make or receive calls on either RMF or personal mobile phones when driving on RMF business (including when used with appropriately fitted hands free car kits) except when the vehicle is parked and stationary with the engine turned off, or in an emergency (i.e., when it would not be possible to stop and make a call) in which case appropriate hands-free equipment must be used.
e) Users should check their company mobile phone for messages regularly.
f) If Users are undertaking a long journey on RMF business, they should check their company mobile when safe to do so, e.g., at a service station (but not in an unsafe area such as a petrol station forecourt) or when at their destination and after returning to the place of work.

## 5) Use of Internet and Social Networking Sites

a) RMF provides access to the internet for the sole purpose of business and to assist Users to carry out their duties. RMF does not allow the internet to be used for personal purposes during working hours.

b) **Authorised Internet Users**

Where a User has been provided with a computer with internet access at their desk, they may use the internet at work. Not everyone in RMF needs access to the internet at work. Anyone who does not have access but believe that they require it should contact their Line Manager and make a written request, setting out the reasons why access should be allowed.

c) **Sensible Internet Use**

i. Where Users are allowed access to the internet at work, they are expected to use it sensibly and in a manner that does not interfere with the efficient running of the foundation. For example, where it would be quicker to make a telephone call than to engage in an internet search for the required information, then the telephone call should be made.
ii. Users may be called upon to justify the amount of time they have spent on the internet or the sites that they have visited.

d) **Removing Internet Access**

The foundation reserves the right to deny internet access to any User at work, although in such a case it will endeavour to give reasons for doing so.

e) **Registering on Websites**

Many sites that could be useful for the foundation require registration. Users wishing to register as a user of a website for work purposes are encouraged to do so. However, they should ask their Line Manager before doing this.

**f) Licences and Contracts**

i. Some websites require the foundation to enter into licence or contract terms. The terms should be printed off and sent for approval to the Line Manager in advance before a User agrees to them on RMF's behalf.
ii. In most cases, there will be no objection to the terms, and it is recognised that the free information provided by the website in question may save RMF money.
iii. Users should, however, always consider whether the information is from a reputable source and is likely to be accurate and kept up to date, as most such contract terms will exclude liability for accuracy of free information.

**g) Downloading Files and Software**

i. Users should download files only onto PCs with virus checking software and should check how long the download will take.
ii. Users should not download software from the internet unless first given permission by IT support staff. If there is any uncertainty as to whether the software is virus-free or whether the time the download will take is reasonable, the relevant Line Manager should be consulted.

**h) Personal Use of the Internet**

i. Although the email system is primarily for business use, RMF understands that Users may on occasion need to use the internet for personal purposes.
ii. Users may access the internet at work for personal purposes provided that:

- Such use is not during working hours
- The internet is not used to access offensive or illegal material, such as material containing racist terminology or nudity

- They do not enter into any contracts or commitments in the name of or on behalf of RMF
- They do not arrange for any goods ordered on the internet to be delivered to the foundation's address or order them in the foundation's name

**i) Use of Professional Social Networking Sites**

i. RMF staff may, with the authorisation of their Line Manager, access professional networking sites such as LinkedIn and such activity may be actively encouraged as a means of marketing your expertise and experience or the foundation.
ii. In using such sites users are acting in their capacity as an employee of RMF and must ensure that profiles and online activities are in accordance with RMF policies.
iii. RMF has proprietary rights over the contents of online networking connections in accordance with the Copyright and Rights in Databases Regulations 1997.

**j) Use of Personal Social Networking Sites**

i. RMF recognises that many Users use the internet for personal purposes and that many Users participate in social networking on websites such as Facebook, Twitter and Instagram amongst others.
ii. As outlined in RMF's Child Protection and Safeguarding Policy and Procedure, RMF staff must NOT use personal networking sites to contact any service user or attendee of RMF programmes.
iii. RMF respects an individual's right to a private life. However, the foundation must also ensure that confidentiality and its reputation are protected. Users must recognise that anything posted online is, by nature, public and that consequences may result from their conduct online. RMF therefore requires Users using personal social networking sites to:

- Refrain from identifying themselves as working for RMF with the exception of social networking for business (such as LinkedIn) and which has been approved by RMF.
- If participating in any personal blog or online forum, ensure that any views and opinions expressed cannot be misunderstood as representing RMF's views.
- Ensure they do not conduct themselves in a way that is detrimental to RMF.
- Refrain from making derogatory or discriminatory comments about RMF, their colleagues or RMF's customers or attendees on such sites.
- Refrain from using networking sites to disclose personal data about colleagues.
- Take care not to allow interaction on these sites to damage working relationships between members of staff, customers or attendees of the foundation.

iv. Users should be aware that inappropriate use of social media in work and private time could constitute Gross Misconduct.

## 6) Online Viewing and TV

a) RMF premises are not covered by a TV Licence.
b) RMF staff, contractors and visitors may not watch or record live TV or BBC programmes on online platforms such as BBC iPlayer on RMF premises on any devices provided by RMF.
c) Staff, contractors and visitors may watch live TV or BBC programmes on iPlayer on their own personal devices provided that the device is powered by internal

batteries and is not plugged in, they have a current TV Licence at their home address, and they are doing so as part of their work.

d) As RMF premises are not covered by a TV Licence, it is a criminal offence for anyone here to watch or record live TV programmes on any channel or device, or to download or watch BBC programmes on iPlayer, without being covered by a licence. There is risk of prosecution and a fine for anyone committing an offence.

## 7) Email

a) Any RMF business which is conducted via email must be conducted through the foundation's email and is under no circumstances to be conducted through another personal email address or account.

### b) Content of Emails

i. Emails that Users intend to send should be checked carefully. Email should be treated like any other form of written communication and what is normally regarded as unacceptable in a letter is equally unacceptable in an email communication.

ii. The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. In serious cases this could be regarded as Gross Misconduct and lead to dismissal.

iii. If a User receives an obscene or defamatory email, whether unwittingly or otherwise, from whatever source, they should not forward it to any other address.

iv. Statements to avoid in emails include those criticising the foundation's competitors or their staff, those stating that there are quality problems with goods or services of suppliers or customers, and those stating that anyone is incompetent.

### c) Copying Others In (using cc)

Users should exercise care not to copy emails automatically to all those copied into the original message to which they are replying. Doing so may result in disclosure of confidential information to the wrong person.

### d) Attachments in Emails

i. Users should not attach any files that may contain a virus to emails as the foundation could be liable to the recipient for loss suffered. RMF has virus-checking in place but, if in doubt, Users should check with their Line Manager or IT support.

ii. Users should exercise extreme care when receiving emails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

### e) Personal Use of Email

Although the email system is primarily for business use, RMF understands that Users may on occasion need to send or receive personal emails using their work address. When sending personal emails Users should show the same care as when sending work emails.

## 8) Security

a) The integrity RMF's business relies on the security of its communications equipment and systems. Access to certain websites may be blocked from RMF communications equipment and systems. Often a decision to block a website is based on potential security risks that the site poses.
b) Users bear the responsibility of preserving the security of communications equipment and systems through careful and cautious use as outlined below:

i. Users must not attempt to circumvent any blocks placed on any website by RMF.
ii. Users must not download, transfer or install any software or program without the express permission of their Line Manager and IT support.
iii. Users must not share any password that they use for accessing RMF communications equipment and systems with any person, other than when it is necessary for maintenance or repairs by IT support staff. Where it has been necessary to share a password, the User should change the password immediately when it is no longer required by contacting the IT support staff.
iv. Users are reminded that it is good practice to change passwords regularly.
v. Users must ensure that confidential and sensitive information is kept secure. Workstations and screens should be locked when the User is away from the machine, hard copy files and documents should be secured when not in use and caution should be exercised when using mobile phones outside of the workplace.
vi. No external equipment or device may be connected to or used in conjunction with RMF equipment or systems without the express permission of the Line Manager.
vii. Care should be taken in the transportation, storage and security of RMF mobile devices (including USB storage devices). Loss of ICT equipment may, depending on the circumstances, result in disciplinary action.
viii. All software on RMF ICT equipment must only be used for the purpose it has been provided and within the terms of the software license.
ix. Users must not reproduce software or use in a way that contravenes its license.
x. Users should seek advice and guidance from their Line Manager and/or IT support staff if they believe something may breach the integrity of RMF's ICT security.

## 9) Safeguarding and Remote Education During Coronavirus

a) For hosting and joining video-conferencing calls the following general rules apply:

i. Be clear about why you are having to make a video conferencing call.
ii. Ensure there is an audit trail and are you aware of RMF's disclosure policies.
iii. Ensure you have parental agreement if the call includes children.
iv. If children are involved there should wherever possible be two members of staff. If not, only Heads of Department should be on the call
v. Only in exceptional circumstances should the call be done from a member of staff's home and always be mindful of your surroundings and what is on view
vi. Do not make the calls public. Connect directly to the people you want to call using your contacts/address book or provide private links to the individual contacts. For some video conferencing services, you can set up the call so that a password is required in order to join. This adds another layer of protection. Do not post the link (or the password) publicly.
vii. Know who is joining your call. If you are organising the call, consider using the lobby feature to ensure you know who has arrived. This is especially useful if individuals are joining the call via an unrecognised phone number. Make sure

people are who they say they are before they join the call (the password function described above can help with this).

viii. Consider your surroundings. Take a moment to think about what your camera shows when you're on a call. Would you want to share that information with strangers? Consider blurring or changing your background - you'll find instructions on how to do this on the support website for your video conferencing service.

b) For further guidance safeguarding procedures when planning and teaching remotely during the Coronavirus (COVID-19) outbreak, visit the Government website:

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19?priority-taxon=b350e61d-1db9-4cc2-bb44-fab02882ac25#communicating-with-parents-carers-and-pupils

## 10) Monitoring

a) RMF may monitor communications in order to:

i. Ensure RMF's policies and guidelines are followed and standards are maintained.
ii. Provide evidence of transactions and communications.
iii. Combat unauthorised use of RMF ICT equipment/systems and maintain security.
iv. Better understand RMF's requirements for ICT equipment and systems.
v. If the User is absent for any reason and communications must be checked for the smooth running of RMF's activities and business to continue.

b) Users should be aware that all internet and email traffic data sent and received using the foundation's communication systems is logged, including websites visits, times of visits and duration of visits. Any personal use of the internet will necessarily therefore be logged also.

c) By using RMF's communications equipment and systems for personal use, Users are taken to consent to personal communications being logged and monitored by RMF. RMF will ensure that any monitoring of communications complies with the relevant statutory requirements (Data Protection, Telecommunications Act etc.).

d) When monitoring emails, RMF will, save in exceptional circumstances; confine itself to looking at the address and heading of the email. Users should mark any personal emails as such and the sender to do the same. RMF will avoid, where possible, opening emails clearly marked as 'private' or 'personal'.

## 11) Misuse and Compliance

Any User found to be misusing RMF ICT equipment and systems will be treated in line with RMF disciplinary procedure which could result in sanctions being applied up to and including dismissal.

## 12) Policy Review and Related RMF Policies

a) RMF regularly reviews policies or procedures to reflect changes in legislation or practice.

b) Policies related to RMF's ICT Usage Policy include:

- RMF Child Protection and Safeguarding Policy and Procedure
- RMF Data Protection Policy
- RMF Staff Disciplinary Policy and Procedure