Document Title	**Mobile Phone Policy (including any other mobile connections or accessed by Group provided connections)**
Type of document	Corporate
Brief summary of contents	• Clear guidance in the use of RNN Group provided mobile connections • Guidance on best practice for use of 'smart' devices • Responsibilities of individuals
SLT member responsible for policy	Director of Strategic Planning & Corporate Service
Date written	22nd June 2017
Date last revised	30th January 2023
This document replaces	NNC Policy on the use of College mobile phones, RC Personal mobile phone/Device usage policy, DVC mobile phone loan agreement
Approval route/consultation	Department Head, SLT Member
Head of Department (HOD) responsible for policy	Kelly Condon
Author of policy	Data Protection Officer
Contact details	DPO@rnngroup.ac.uk
Publication location	Public and portals
Date of final approval	31st July 2017
Date policy becomes live	1st August 2017
Review period	Annual
Links to external standards	ICO, relevant Acts of Parliament as detailed within the policy
Related documents	• BYOD Policy • Data Protection Policy • DSAR Policy • Staff Acceptable Use Policy • Privacy Policy
Keywords	Telephone, Mobile, Texting, Device, Connection, IT, ICT, Technology, BYOD, Email, Internet, Data Protection, Legislation, Password
Training needs	Data Protection

This document is only valid on the day of printing

Mobile Phone Policy

Version 1.3

30th January 2023

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
22 June 2017	1.0	Birth of policy	Ian Headley
8th May 2018	1.1	Minor update for data protection legislation changes	Ian Headley
4th November 2019	1.2	Minor changes in password creation and job titles and annual review	Kelly Condon
30th January 2023	1.3	Annual Review	Kelly Condon

All or part of this document can be released under the Freedom of Information Act 2000

Table of Contents

Appendices

Policy Outline

The ability of employees to use telephony services, texting services, email and access to the Internet on Group provided mobile devices provides new opportunities for the RNN Group (Hereinafter referred to as the 'Group') as it facilitates the gathering of information and communication with fellow employees, customers and other contacts whilst outside normal operating premises.

It is recognised that in certain circumstances, personal devices may need to contain Group SIM cards, this policy will apply to any usage in these circumstances. The security requirements outlined within this policy must also be met on that device, this may include the encryption of that device to Group standards and the requirements for password as stipulated below.

However, any telephone usage, text services, Internet and email access (this is not an exhaustive list, all mobile related equipment and services should be considered) opens the Group to new risks and liabilities. It is therefore essential that relevant employees read these guidelines and make themselves aware of the potential liabilities involved in using mobile phones and other mobile connections provided by the Group.

The Group monitors ALL Internet access on ALL RNN Group provided equipment. This includes monitoring activity even when services are provided by a third-party Internet provider.

Any Internet access or services on the Internet are subject to the staff Acceptable Use Policy (AUP) and that policy should be read in conjunction with this.

The aim of this policy is to give staff a framework within which to carry out their duties in a way that might prevent possible legal redress or disciplinary action.

All relevant users will be provided with a copy of this policy. It is the end user's responsibility to read and understand the terms of this policy when they are supplied with a mobile device or mobile connection from the Group.

Acceptance to this policy will be demonstrated on the Equipment Loan Agreement form, (a copy of which can be found in Appendix 1) which will also detail the type of connection and/or device being supplied by The Group.

1. General Points

1.1 Use of Group provided mobile telephones or any other mobile connections, is primarily for work-related purposes. This includes the use of any device which contains a Group SIM card and/or other device connection.

1.2 Any mobile devices containing Group owned SIM cards (including the use of these SIM's in personal devices) are subject to this policy. This policy also applies if a personal device is accessing Group systems in any way e.g. email access on the personal device.

1.3 The Group has the right to monitor any and all aspects of its telephone and computer systems that are made available to you and to monitor, intercept and/or record any communications made by employees, including mobile

telephones, in line with current legislation. ***See section 11.***
Consent for this type of monitoring is not required as processing of this data is performed as a legitimate business interest and may be processed in the public interest.

1.4 Mobile devices and the data stored on, or transmitted from, are the property of the Group and are designed to assist in the performance of duties. Employees should therefore, have no expectation of privacy in any data stored, sent or received, whether it is of a business or personal nature.

1.5 It is inappropriate in the use of Group provided connections (and use of the Internet) for employees to access, download or transmit any material that **might intentionally or unintentionally damage the interests of The RNN Group, its students, employees or other stakeholders. Obscene, abusive, sexist, racist or defamatory material shall be included within this category**.

1.6 Staff requiring further clarification of the above should contact the Head of IT Services and/or the Deputy Head of IT Services. Employees should be aware that such material may also be contained in materials such as jokes, stories or articles sent via email or text.

1.7 Such misuse of systems will be treated as misconduct and may, in certain circumstances, be treated by the Group as gross misconduct.

1.8 The Group reserves the right to use the content of any employee mobile device usage to form part of any disciplinary process or proceedings.

2 Use of Services

2.1 Email - The staff Acceptable Use Policy (AUP) details the conditions for use of emails and is applicable to this policy. Staff are reminded to read this section of the staff AUP to ensure compliance.

2.2 Internet - The staff AUP details the use of the Internet and is applicable to this policy. Staff are reminded to read this section of the staff AUP to ensure compliance.

2.3 Copyright and downloading - The staff AUP details the conditions for the use of copyrighted material and Internet downloads and is applicable to this policy. Staff are reminded to read this section of the staff AUP to ensure compliance.

2.4 Premium rate – Under no circumstances should any Group provided connection be used to access premium rate services.

2.5 Telephone billing analysis is performed on a monthly basis and any excessive costs may be queried with the end user at any time. Users should therefore be in a position to provide further details of calls and/or other usage upon request. Excessive use may lead to investigations and action under the Group Disciplinary Procedure.

3 "Pay as you go" (PAYG) Telephones

3.1 Pay as you go telephones are only issued and used in an emergency situation, these devices will be supplied by IT Services as and when the need arises. Any top ups required for the PAYG device must first be authorised by IT Services and, where applicable, the CEO & Principal or Deputy CEO and Principal, as prescribed within the Group financial regulations.

4 Security

4.1 There is an expectation that the end user will password protect their device whatever the circumstance, if the device is a non-smart device and not possible to be protected via Mobile Device Manager (MDM), a minimum expectation is for the device to be PIN coded for security (as complex as possible). All smart devices that contain a Group connection must be added to the Group's MDM software to encrypt and protect the device along with the data stored on same.

4.2 Employees are responsible for safeguarding their passwords for the Group's systems. For reasons of security, individual passwords must not be written down, printed, stored on-line or given to others. User password rights given to employees should not give rise to an expectation of privacy.

4.3 Passwords are an important aspect of computer security and are the primary authentication method for access to IT resources. The Group's standard for password creation is set to a minimum of 16 characters with a mixed combination of upper and lower case letters, numbers and special characters included. This password structure will be maintained by the individual on the mobile device provided.

4.4 Where possible, auto-lock of each device must be set to a maximum of 5 minutes of inactivity and should be set to a shorter interval wherever possible and practicable.

4.5 If an individual is accessing Group resources (e.g. email), on a personal device then that device must be encrypted to the latest available standard for the device and operating system, as is required on RNN Group owned devices. Guidance on encrypting personal devices is readily available on the Internet.

4.6 Personal Identifiable Information (PII) must never be stored on a mobile device whether Group or personally owned.

5 Use of Mobile Devices Whilst Driving

5.1 Since 1st December 2003, it has been a criminal offence to use a phone whilst driving or riding a motorcycle unless hands free access (as defined by the UK Government) is used such as:

- A Bluetooth headset
- Voice command
- A dashboard holder

- In car manufacturer installed or retrofit hands-free systems

The law still applies if you are:

- Stopped at traffic lights
- Queuing in traffic
- Supervising a learner driver
- Stationary on a public highway

5.2 If a hands free, system is used then full control of the vehicle must be maintained at all times (Highway Code rule 149).

5.3 The Police can stop an individual if they suspect that the individual is not in control because the individual is distracted and the individual may be prosecuted. The Group accepts no responsibility for any Police action taken against any individual.

5.4 Subject to the legislation in force at any given, a hand-held phone may only be used if either of these conditions apply:

- The vehicle is safely parked
- There is an urgent need to call 999 or 112 in an emergency and it's unsafe or impractical to stop

6 Software Installation

6.1 All software for use on mobile devices must be purchased through, and installed by, the IT Services department.

6.2 It is a criminal offence, and contrary to the Group's staff AUP, to install software for which the Group is not is possession of a bona fide licence.

7 Data Protection

7.1 Data Protection legislation regulates the collection and processing of personal and special categories of data, there is an expectation that data of this nature is not stored on any device owned by the Group, or within a device that has a Group provided connection, that is not encrypted. It is the individual's responsibility that all aspects of the Data Protection legislation and the Group's Data Protection Policy are adhered to when using Group provided mobile connections.

7.2 Sensitivity should be observed when discussing confidential issues over a mobile connection. It is therefore recommended that highly sensitive discussions be organised face to face rather than over the telephone or done in a secure, private location.

7.3 No cloud storage providers should be synchronised with the mobile device itself other than the Group provided Office 365 and Google Drive accounts. The user should ensure this type of service is turned off on the device if it is not being used.

8 Mobile Device User Agreement

8.1 All users will be provided with a copy of this policy before they are supplied with a Group mobile device or connection. It is the end user's responsibility to read and understand the contents. Devices are provided to the individual for the individuals use only, each user will be expected to sign the Group equipment loan form before any equipment is issued to them.

9 Damage or Loss

9.1 Where a mobile device (or Group provided mobile accessories) is damaged, lost or stolen through carelessness, the individual to whom the device has been assigned may be responsible for the cost of the replacement device either directly or through appropriate insurance.

9.2 It is the individual's responsibility to ensure that IT Services are informed as soon as the individual becomes aware should a device, SIM or other provided connection be lost or stolen to enable temporary blocking to be activated. This must be done as soon as practicable and in any event within 24 hours (subject to weekends and Group closure days) of the discovery of loss etc. without exception. This includes any loss of personal equipment where an RNN Group provided SIM card has been provided and is being used.

10 Linked Policies and Guidance

Policies and guidance linked to this policy:

- Staff Acceptable Use Policy (AUP)
- BYOD AUP
- Data Protection Policy
- Data Subject Access Request (DSAR) Policy
- Privacy Policy

11 Legislation

Legislation covered in this policy:

The Investigatory Powers Act 2016 (previously known as The Regulation of Investigatory Powers Act 2000 (RIPA))
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Regulations)
The Data Protection Act 2018
The Freedom of Information Act 2000
The Human Rights Act 1998
The Privacy and Electronic Communications (EC Directive) Regulations 2003 and amendment to the Regulations 2011
The Counter-Terrorism and Security Act 2015
The Computer Misuse Act 1990
The Terrorism Act 2006
The Police and Justice Act 2006
The Copyright, designs and Patents Act 1988

The Equality Act 2010
The Limitation Act 1980
The Malicious Communications Act 1988
The Digital Economy Act 2017
The Prevent Strategy 2011

Appendix 1:

Equipment Loan Agreement

Agreement of loan between

RNN Group, Eastwood Lane, Rotherham S65 1EG

And

Name : …….

Site : ……

Provision of equipment

1. All loaned equipment remains the property of the RNN Group and must be returned in the same condition in which the equipment was supplied to the individual under this agreement. The working condition of the equipment will be assessed upon its return.

2. The individual identified above is solely liable for the equipment listed in the schedule until they return it to IT Services and must notify the IT Services department of ANY damage to the equipment, accidental or otherwise at the earliest possible opportunity, within 24 hours in ALL instances.

3. The named individual is responsible for ensuring all equipment is stored securely and safely at all locations.

4. The following guidelines must be adhered to at all times:
    a. No additional hardware, peripheral or software is to be added to, removed from, or installed on the loaned device unless express permission is obtained from the RNN Group Head of IT Services or Deputy Heads in his absence.
    b. The RNN Group will not be held accountable for any unauthorised copying of software.
    c. All reasonable precautions must be taken by the individual to ensure the safety of the equipment provided at all times.

5. The named individual is required to report any problems experienced with the equipment on the RNN Group's Helpdesk (https://helpdesk.rnngroup.ac.uk) during the loan period.

6. All maintenance and support for the loaned device will be solely provided by the RNN Group IT Services department.

7. If the borrower does not return the equipment when requested or on cease of employment, then this will be reported to the HR department for follow up action. This action may result in the individual being responsible for the full replacement cost of the device should this be deemed necessary.

8. The above named individual must not cause any form of damage to the RNN Group's equipment or software. The term 'damage' includes modifications to hardware or software, which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Costs associated with repairing or replacing the damaged equipment or software and/or providing temporary replacements may be charged to the person or persons causing the damage. The costs will be determined by the Group themselves.

9. The equipment provided has been designed to provide a consistent service, adequate user support and where applicable, network compatibility and should not be altered in any way.

10. The equipment listed will be reset upon return and therefore all content stored within the device will be erased and no longer be available. The individual is responsible for performing their own backups prior to returning the device to IT Services.

11. The RNN Group is not responsible for any files left on a loan device or for a loss of, or damage to, the individuals files during the loan period. The Group is also not responsible for any computer viruses transferred to or from an individual's external storage whilst using the equipment.

12. In using RNN Group provided equipment, the individual is agreeing to its use within the detail of the relevant Acceptable Use Policy (AUP).

13. All equipment must be provided to IT Services for checking when requested to ensure adherence to this agreement.

14. Staff will be required to produce their RNN Group ID, prior to any equipment being released to them.

Duration and termination of agreement

1. This agreement shall come into force on the day of the individual signing acceptance of the equipment for a period of no longer that three years or until the named individual leaves the employment of the RNN Group, whichever is sooner.

2. This agreement shall be terminated should the named individual fail to adhere to any of the conditions stipulated above or any conditions within their contract of employment with RNN Group.

3. This agreement can be terminated with immediate effect should the equipment no longer be utilised or required by the individual. It must be returned to IT Services and not passed to another member of staff.

Data Protection

No Personal Identifiable Information (PII) is to be stored on portable devices owned by the RNN Group, including but not restricted to laptops, tablets and mobile phones. Group encrypted devices are however, acceptable for PII storage, subject to the relevant data retention periods.

IT Services contact details

Helpdesk email : helpdesk@rnngroup.ac.uk

Loan equipment telephone contact : 01709 722783

Linked policies

Staff Acceptable Use Policy (AUP)

Data Protection Policy

Mobile Phone Policy

Authorisation of agreement

Period of agreement			
From		**To**	
Signatories			
IT Services staff member name			
IT Services staff member signature			
Date			
Individual accepting loan equipment			
Name			
Signature			
Date			
In signing this document, I agree to abide by the terms and conditions of this loan stipulated above. I have checked that the equipment is operational and understand that all equipment will be reset on return. *I also understand that the physical security of the equipment listed is my responsibility and I shall report loss of device or any faults as and when they occur.*			

The RNN Group is what's known as 'the controller' of the personal data you provide to us.

We need to know your basic personal data in order to provide you with details regarding your interaction with the RNN Group, it will also be used by the Group's analysis services, where appropriate. We will not collect any personal data from you that we do not need in order to provide and oversee services to yourself.

We have a Data Protection regime in place to oversee the effective and secure processing of your personal data. We shall not disclose the information you entrust us with to third parties except where we have a statutory or contractual duty to do so (including to your employer, if sponsored), where you have given prior approval or where an official RNN Group third party data sharing agreement exists.

The RNN Group will use your name and email address to inform you of our future offers and similar products or services. This information is not shared with third parties and you can unsubscribe at any time via phone, email or on our website.

If at any point you believe the information we process about you is incorrect, you can request to see this information and even have it corrected or deleted, simply email sar@rnngroup.ac.uk outlining your specific requirements.

If you wish to raise a complaint on how we have handled your personal data, you can contact our Data Protection Officer who will investigate the matter for you, please email dp@rnngroup.ac.uk with full details of the complaint.

More information on the RNN Group Data Protection framework can be found on our website.

Appendix A

Equipment Loan Agreement

Equipment loaned to :

.....

Delivery				**Return**	
Date	**Item Description**	**Asset Number**	**Signature**	**Date**	**Signature**

Version 1.1, 30th November 2017