Document Title	Mobile Phone Policy (including any other mobile connections or accessed by Group provided connections)
Type of document	Corporate
Brief summary of contents	To provide: • 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	Tony De'Ath
Date written	22nd June 2017
Date last revised	4th November 2019
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	Chris Muffett

Author of policy	Ian Headley
Contact details	ianheadley@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 • AUP 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 1.2

4th November 2019

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
22/06/2017	1.0	Birth of policy	Ian Headley
08/05/2018	1.1	Minor update for data protection legislation changes	Ian Headley
04/11/2019	1.2	Minor changes in password creation and job titles. 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 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 RNN 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 RNN 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 RNN 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 this 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 users responsibility to read and understand the terms of this policy when they are supplied with a mobile device or mobile connection from the RNN Group.

Acceptance to this policy will be demonstrated on the Equipment Loan Agreement form, which will also detail the type of connection and/or device being supplied by The Group.

1. General Points

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

1.2 Any mobile devices containing RNN 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 RNN Group systems in any way e.g. email access on the personal device

1.3 The RNN 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 needed 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 use of RNN 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 or employees. Obscene, abusive, sexist, racist or defamatory material is included within this category**.
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 jokes sent by email or text.
Such misuse of systems will be treated as misconduct and may, in certain circumstances, be treated by The Group as gross misconduct.
The RNN Group reserves the right to use the content of any employee mobile device usage in any disciplinary process.

2 Use of services

2.1 Email - The staff 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 an RNN 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 RNN 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 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/Principal, within the RNN 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 an RNN Group connection must be added to the RNN 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 should not be 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. 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.

4.5 If you are accessing RNN 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 easily available on the Internet.

4.6 Never store Personal Identifiable Information (PII) on a mobile device whether RNN Group or personally owned.

5 Use of mobile devices whilst driving

5.1 As from 1st December 2003, it is a criminal offence to use your phone while driving or riding a motorcycle unless you have hands free access (as defined by the UK Government) such as:

- A Bluetooth headset
- Voice command
- A dashboard holder

The law still applies if you are:

- Stopped at traffic lights
- Queuing in traffic
- Supervising a learner driver

If you use your hands free, you must stay in full control of your vehicle at all times (Highway Code rule 149).

The Police can stop you if they think you are not in control because you are distracted and you can be prosecuted. The RNN Group takes no responsibility for any Police action taken against individuals.

You can use a hand held phone if either of these conditions apply:

- You are safely parked
- You 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 of mobile devices must be purchased through, and installed by, the IT Services Department.

6.2 It is a criminal offence, and contrary to the RNN Group's 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 RNN Group provided connection, that is not encrypted. It is the individual's responsibility that all aspects of the Data Protection legislation and the RNN 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 account. 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 RNN Group mobile device or connection. It is the end users 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 RNN 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, staff 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 within 24 hours of the discovery of loss etc. without exception. This includes any loss of personal equipment where a 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

11 Legislation

Legislation covered in this policy:

Investigatory Powers Act 2016

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Regulations)

The Data Protection Act 2018

Freedom of Information Act 2000

The Human Rights Act 1998

The Privacy and Electronic Communications (EC Directive) Regulations 2003

The Counter-Terrorism and Security Act 2015

The Computer Misuse Act 1990

The Terrorism Act 2006

Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

Police and Justice Act 2006

Copyright, designs and Patents Act 1988

Equality Act 2010

Limitation Act 1980

Malicious Communications Act 1988

Digital Economy Act 2017

Prevent Strategy 2011