Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Policy Title: Joint Mobile Computing & Remote Access Policy

Reference	POL/IG/012
Version	V2.0
Date Ratified	19/03/2019
Next Review Date	31/03/2022
Date published	28/05/2019
Accountable Director	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)
Policy Author	Trust Information and Cyber Security Officer

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Policy On A Page

SUMMARY & AIM

This policy provides direction on the use and care of mobile and hand held computing devices used throughout Cumbria Partnership NHS Foundation Trust (CPFT) and North Cumbria University Hospitals NHS Trust (NCUHT). This is to ensure compliance with the relevant standards and legislation.

Users must always comply with the rules laid down in this Policy when using Trust mobile information processing facilities. Users must also remember that, it is not just in electronic processing, but in verbal and written communication, occurring in public areas, that risk is involved and breaches may occur.

TARGET AUDIENCE:

- All Trusts' employees, consultants, third parties, contractors and temporary workers using Trusts' systems
- All Partner Organisations delivering services on behalf of the Trusts and using Trusts' systems and others who have been given access to internal Trusts' systems in support of service delivery.

TRAINING:

- Employee Induction
- Mandatory Data Security Awareness training using the Trust TNA eLearning programme option: 261 – 0000 Data Security Awareness Level 1

KEY REQUIREMENTS

1. Users must always comply with the rules laid down in this Policy when using Trust mobile information processing facilities.

2. Users must also remember that, it is not just in electronic processing, but in verbal and written communication, occurring in public areas, that risk is involved and breaches may occur.

3. Ensure the safekeeping of the hardware, software and data held on the computer; and any relevant hard copy data whether in the office, travelling between work locations or at home.

4. Users are reminded that with any encrypted device no password/username or other access control information is to written down and stored with the device.

5. Understand the standards to be adhered to when using portable devices such as laptop and notebook computers; and for any other movement of information from its normal location to another site.

6. Managers must ensure all staff members are aware of and in compliance with this Policy.

7. Managers must also ensure that any potential disciplinary action with regard to the use or misuse of mobile information processing facilities is investigated with this and other relevant Policies in mind.

TABLE OF CONTENTS

1. INTRODUCTION

Information held in electronic information systems within the Trusts represents one of the Trusts' most valuable assets. It is, therefore, essential that all computers, networks and information contained within them are protected against the many threats which may compromise the data, patient or staff privacy.

Demands on services vary but the scope of providing services that meet each organisation's requirement for information system security remains the same. Each organisation (i.e. The Trusts and any contractors) must recognise and accept their responsibilities for the security of their assets.

The use of laptops, notebooks, tablets and smartphones (mobile devices), increases the risks associated with the secure storage, movement and processing of data. The purpose of this Policy is to set out the criteria for the provision of mobile devices and the conditions relating to their use.

2. PURPOSE

This document sets out the organisations' Policy for the protection of the confidentiality, integrity and availability of their assets whilst using portable mobile devices.

The objective of this document is to define the standards to be adhered to when using portable mobile devices such as laptop and notebook computers; and for any other movement of information from its normal location to another site for staff to work with that data.

It therefore supports and is supported by other policies and procedures dealing with specific functional areas and requirements such as Acceptable Use, Forensic Readiness and the Management of Risk.

3. POLICY DETAILS

Computer and information security is the responsibility of the user at all times. It is the user's responsibility to ensure the safekeeping of the hardware, software and data held on the computer; and any relevant hard copy data whether in the office, travelling between work locations or at home.

This document details the standards that must be adhered to by staff when removing data from its normal place of storage to another location, in order for that member of staff to work on that data (whether that location is a Trust site, another organisation's site or the staff member's home).

Where sensitive information is being processed the data device used must be a Trust-supplied device, and cannot be another organisation's device or the staff member's own computer. Media should normally be Trust-supplied. Images, pictures and video are included within the definition of 'data'.

It is the policy of the Trusts that users of mobile devices must comply with all current legislation and local policy that relates to the use and retention of patient information and the use of computer systems. These include but are not limited to:

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act, 1990.
- The Copyright, Designs and Patents Act, 1998.
- Access to Health Records Act, 1990.

Failure to do so may lead to withdrawal of access to mobile devices, and disciplinary action taken against the individual(s) concerned. Where violation of these conditions is deemed to be illegal, the matter may lead to criminal prosecution.

3.1 Mobile Devices

The Trust will consider the provision of a mobile device if the following criteria are met:

- a member of staff is required to work from more than one location and convenient access to a desktop PC is not available in all the locations;
- a member of staff regularly undertakes work at home on behalf of the Trusts, provided that such work does not breach the European Working Times Directive.

Requests for mobile devices must be made to the Line Manager and submitted to the IT Service Desk, who will progress the request. The member of staff's department may be responsible for meeting the cost of the provision of the mobile device, which must be approved in advance by the appropriate budget holder.

3.2 Remote Access via the Virtual Private Network (VPN)

All staff members wishing to work with Personally Identifiable Data or Business Sensitive information at home must submit a formal request via the IT Service Desk (CPFT) or by completing and submitting an 'Offsite Request & Authorisation form' (NCUH). This form is available on the Trusts Intranet site http://nww.staffweb.cumbria.nhs.uk/it/forms/HomeWorkingRequestForm.pdf

N.B. *No offsite working will be allowed until the IT Service Desk process (CPFT) or a duly authorised form (NCUH) is received back by the requester.*

Where there is an authorised requirement for a user to work away from NHS premises, remote connectivity is only to be used via the Trusts' VPN. Use of the VPN system requires that users are issued with a Secure Remote Access PIN.

It is a user's responsibility to ensure that any security mechanisms, used to gain access to the VPN, are kept safely and securely. PINs must be kept confidential and not disclosed to anyone. Users are to be aware of the following:

- **Never** keep written notes of usernames, passwords, PINs or other access credentials.
- The Trusts primarily use an SMS based system which is used in conjunction with the users work phone. These should be kept separate from the laptop device
- Credentials must not be shared between users and must not be transferred to other members of staff unless by the IT team.
- Credentials that become surplus to requirement must be notified to the IT Service desk as soon as they are no longer required and arrangements for their recovery will be made.

N.B. If a user does not log in to the VPN system for three months their remote access privileges will be removed. It will only be reinstated on completion and submission of another remote access VPN request form. The only exceptions to this will be devices used for business continuity and managers requiring on-call access.

3.3 Conditions Attached to the Provision of Mobile Devices

The provision of Trust mobile devices and shall be subject to the following conditions:

3.3.1 Personally Identifiable Data (PID)

In order to comply with the General Data Protection Regulation and the recommendations of the Joint Information Governance Board, Personally Identifiable Data shall be stored on a mobile device only when this is absolutely and operationally necessary. Where this is the case, the following conditions apply:

- Such storage must be Lawful, Fair and Transparent in line with GDPR requirements
- It must be for a limited and specific purpose
- It must be accurate
- Data shall be stored only for the time period when it is actively being used
- Data shall be deleted immediately after use
- Data minimisation
    - only the minimum amount of personally identifiable data, necessary for the current purpose, shall be stored
    - the person's name shall be stored only when absolutely necessary
- For tasks involving personally identifiable data from locations within the Trusts, users will be required, wherever possible, to use the Trusts' network to store data
- Photographs of PID are not to be taken by mobile devices (or emailed)
- To ensure accountability storage of PID on a mobile device must be recorded in your Department's Record of Processing Activity (RoPA)

- The device must be owned by the Trust.
- No personal mobile devices can be used for the storage or processing of PID or other Trust sensitive data
- Password authentication must be applied
- Encryption must be applied

3.3.2 Virus Protection and Software Updates

All Trust Laptop devices have up-to-date Anti-Virus software installed at the time they are issued. The anti-virus system's database will be updated on a regular basis. Users must ensure that they make regular connections to the network at least every 30 days to ensure that automatic software patches and antivirus updates are applied to that device.
If a virus is discovered it should immediately be reported to the IT Service Desk and the device and any media used with it, quarantined immediately for inspection and cleaning.

3.3.3 Backups

Mobile devices should not be the primary repository of data, they may be used to hold changes until reconnected to the network and synchronisation can take place with the network storage.

3.3.4 Personal Use

Although limited personal use is permitted, it should be kept to a minimum and used for emergencies only. The Trust accepts no responsibility if personal data that is being stored on a device such as photos, music or software, is deleted or corrupted whilst the mobile device is being repaired or serviced by IT Support staff.

3.3.5 Use of the Internet

The Trusts' Joint Acceptable Use Policy (AUP) covers use of the Internet on Trust mobile devices.

3.3.6 Consumer Devices (e.g. Apple iPads and iPhones)

Users issued with a Trust owned iPad, iPhone or Android device will be connected to their email and calendar functions by use of the Trust's Mobile Device Management (MDM) security system. This ensures security of the data and that there is no interaction with the remainder of the device.

Users are forbidden from attempting to "jailbreak" the device or otherwise seek to alter its security configuration. Users are also forbidden from downloading and installing applications and additional functions to the device. Such requirements must be notified to the IT Service Desk.

3.3.7 The Trust Right to Inspect Data

All data and software held on Trust mobile devices may be inspected by authorised staff at any time and without warning. Such authority must be obtained from the CCIO, CIO or DPO prior to any inspection. Users may be required to remove software and/or data which are deemed to be inappropriate.

3.4 Administration and Support

The configuration of mobile devices will be undertaken by appropriately trained IT staff. Users are not to attempt to resolve issues by themselves. All users will be supported by the IT Service Desk for the following:

- Fault Reporting – Contact by phone, email or alternatively select the hyperlink to the IT Service Desk which is located on the Intranet.
- Maintenance.
- Password resets.
- Requests for access to Trust applications (Alloy, Rio, Strata, ESR etc).

3.5 Using a Mobile Device Away from Trust Premises

When a member of staff is issued with a Trust mobile device there is an implied duty of care and users must take personal responsibility for the security of the equipment, software and data in their care. Any loss, theft or damage resulting from a failure in this duty of care may result in disciplinary action. The safety of staff is the Trust's key priority and if a member of staff is physically threatened then they must give up their mobile device at once. In such cases the Trust will support the individual member of staff in line with the Trust's values. The following measures also apply:

- Users are bound by the same Acceptable Use Policy when operating on Trust premises or working remotely.
- Mobile devices in cars must be stored out of sight when the car is left unattended e.g. in boot.
- When travelling mobile devices (and media) should not be left unattended in public places.
- Mobile devices should be carried as hand luggage when travelling by public transport.
- When the user is away on Trust business mobile devices should be kept out of sight in a locked hotel room or hotel safe.

Where possible, staff should avoid using mobile devices in public places and care must be taken to ensure that there is no risk of overlooking or being overheard. When it is clearly obvious that to continue to work becomes untenable and puts data at unnecessary risk, staff must discontinue and log off.

In the event of theft whilst away from Trust premises, the user must report the incident to the Police immediately and obtain an incident number. Mandated additional reporting measures are detailed Section 3.6 below.

3.6 Losses, Confidentiality & Security Breaches

Any incidents that represent a loss of hardware or data which could potentially lead to breach of confidentiality must be immediately reported, normally to the IT Service Desk in the first instance.

All incidents must be recorded on the Trusts' Incident Reporting System - Ulysses. Incidents could involve, but are not limited to:

- Loss of hardware
- Loss of software
- Loss of data
- Virus attack
- Unauthorised access
- Misuse of system / privileges

Breaches of confidentiality may be reported as a Serious Incidents Requiring Investigation (SIRI) subject to the escalation process defined in the Trusts' Incident Reporting Policies.

3.7 Access Control

All Trust users will have unique, personal Active Directory logon identifiers. All devices will have the required Windows domain authentication enabled on the device. Passwords are to be changed when required (Active Directory forces users by policy to change this password every 60 days).

3.8 Encryption

Mobile devices will be encrypted with the Trust procured encryption product. More details on encryption can be found by contacting the IT Service Desk.

3.9 Data Security

Data must not be stored on the local hard disk (c:/ drive) of mobile devices or saved to the 'Desktop'. It must be stored on a network file store which will save the data securely to the Trusts' file server(s) and from there it will be regularly backed up. Users must make regular connections to the network for security updates and to synchronise data. This will minimise the risk of data loss from use in stand-alone mode.

Where data has to be saved locally to a mobile device, the user should ensure that sensitive data is locally encrypted on the device and backed up at the earliest opportunity. Please see Section 3.3.1.

Advice and guidance can be sought from the IT Service Desk.

4. TRAINING AND SUPPORT

In order to ensure the correct implementation of this policy all managers are required to ensure that all their staff members who have been issued with a mobile device are aware and have understood its content as part of approval of registration applications.

Managers should undertake regular information risk evaluations to be able to demonstrate that staff members' skills and capabilities, with regard to the use of mobile devices are up to date and relevant to the needs of the organisation.

5. PROCESS FOR MONITORING COMPLIANCE

The table below outlines the Trusts' monitoring arrangements for this policy/document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
On-going review of Mobile Device Management concerns and issues highlighted to the Board.	Joint IG Board reviews	Trusts' Cyber Security Officers	Joint IG Board	Quarterly
Information Security Incidents related to Mobile Devices	Ulysses Reports	Head of IG and Trusts' Cyber Security Officers	Joint IG Board	Quarterly
Spot checks on Policy compliance and knowledge	Monthly spot checks – results to be presented to the IG Board	Head of IG	Joint IG Board	Quarterly

Wherever the above monitoring has identified deficiencies, the following must be in place:

- Action plan
- Progress of action plan monitored by the Joint IG Board minutes
- Risks will be considered for inclusion in the appropriate risk registers

6. REFERENCES:

Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents

Computer Misuse Act 1990
http://www.legislation.gov.uk/all?title=computer%20misuse%20act

Employment Practices Code
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Information Security Management NHS Code of Practice
https://digital.nhs.uk/article/1201/Information-security-management-NHS-code-of-practice

Codes of practice for handling information in health & care
https://digital.nhs.uk/codes-of-practice-handling-information

NHS Digital
https://digital.nhs.uk/

National Cyber Security Centre
https://www.ncsc.gov.uk/

7. ASSOCIATED DOCUMENTATION:

Information on the topics listed below can be found on individual Trust Intranet pages. Direct hyperlinks have been removed due to accessibility issues during the integration. If in doubt please contact the Joint IT Service Desk.

CPFT Intranet: http://cptportal.cumbria.nhs.uk/Pages/Home.aspx
NCUHT Intranet: http://nww.staffweb.cumbria.nhs.uk/index.aspx

- Information and Cyber Security Guidance
- Information and Cyber Security Policy
- Information Security Acceptable Use Policy
- Information Risk Policy
- Disciplinary Procedure
- Policy for the Use of Social Networking Sites.

8. DUTIES (ROLES & RESPONSIBILITIES):

8.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trusts, including ensuring that Trusts' policies comply with all legal, statutory and good practice requirements.

8.2 Executive Director of Finance & Strategy (Joint Director of IM&T and Estates):

The Executive Director of Finance & Strategy is responsible for ensuring the development and sign off of this Policy. They ensure the policy is kept up to date by the relevant author and approved at the appropriate committee.

8.3 Senior Information Risk Owner (SIRO) Responsibilities:

The SIRO has responsibility for ensuring that a Mobile Computing & Remote Access Policy is in place, and for assuring the Joint Trust Board of compliance with relevant legislative and mandated requirements. The SIRO has overall responsibility to ensure an Information & Cyber Security Policy framework is in place, including processes to monitor such use, thereby providing assurance that management of threats to security is in place, and that all employees are aware of their responsibilities

The role of the SIRO:

- Is accountable for approving all Information Assets.
- Fosters a culture for protecting and using data.
- Provides a focal point for managing information risk and incidents.
- Is concerned with the management of all information assets.
- To provide a focal point for the resolution and/or discussion of information risk issue.
- Ensure that all care systems information assets have an assigned Information Asset Owner.
- Ensuring the Organisation has a plan to achieve and monitor the right Information Governance culture, across the organisation and with its business partners.
- Approval of all information asset business continuity plans.
- Document a plan for information security assurance that identifies the support necessary to ensure work related to information security management is appropriately carried out.
- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Review and agree action in respect of identified information risks.

8.4 Caldicott Guardian Responsibilities:

The Caldicott Guardian is appointed by the Trust Board and registered with NHS Digital. They ensure that the Trust achieves the highest standards for handling patient information. They represent and champion patient confidentiality issues within the Trust's overall Information Governance Framework

8.5 Business Managers' Responsibilities:

Business Managers must ensure that they have agreed and implemented the departmental arrangements for ensuring compliance with this policy and all policies that are related.

Managers are responsible also for ensuring adequate dissemination and implementation of Policies relevant to the staff in their areas. If applicable, managers must ensure staff can access the hard copy policy summary file on their

ward / department and ensure staff members understand how to access policies on the Intranet.

8.6 Approving Committee Responsibilities: Joint Information Governance Board

The Joint IG Board is the oversight committee for all items relating to information governance and reports into the Joint Clinical Governance Group and Quality and Safety Committee (Board Sub Committees) as required. In terms of policy responsibilities the role of the Joint IG Board is to ensure that local policies compliment the national policy, strategy and guidance relating to information governance and that it is implemented and evaluated appropriately within the Trust. The Joint IG Board are responsible that regular review of information governance policies and procedures takes place and monitors policy compliance at each of its meetings.

The Joint Information Governance Board (JIGB) is responsible for reviewing this Policy, ensuring it is fit for purpose and that it is ratified and passed for publication. The Chair of the JIGB will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree the approval of the final draft of the policy.

The Head of Information Governance reviews Information Governance incidents reported through the Trusts' Risk Management systems with this Policy in mind. The Head of Information Governance reports Serious IG Incidents to the JIGB. To further support the tenets of this Policy the Head of Information Governance reviews the Trusts' Information Flow Mapping on an annual basis, and reports any 'high risk' flows to the JIGB.

8.7 Trust Cyber Security Managers' Responsibilities

The Trust Cyber Security Managers are responsible for:

- Acting as a central point of contact on information & cyber security within the organisations, for both staff and external organisations.
- Implementing an effective framework for the management of security.
- The formulation, provision and maintenance of Information & Cyber Security Policies.
- Advising on the content and implementation of the Information & Cyber Security Programme.
- Producing organisational standards, procedures and guidance on Information & Cyber Security matters for review by the Caldicott Guardians and other senior staff represented on the JIGB, and other Governance Committees, on behalf of the Joint Trust Board,.
- Co-ordinating information & cyber security activities particularly those related to shared information systems or IT infrastructures.
- Liaising with external organisations on information & cyber security matters, including representing the organisations in cross-community issues.
- Ensuring that contingency plans and disaster recovery plans are reviewed and tested on a regular basis.

- Representing the organisations on internal and external bodies that relate to security.
- Ensuring the system, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally.
- Providing an incident and alert reporting system.
- Maintain contact with special Interest Groups in order to:

    - Keep abreast of “best practice”.
    - Maintain current knowledge of security-related matters.
    - Receive early warnings, alerts, advisories, etc. pertaining to developing threats[1].
    - Gain access to specialist advice.
    - Share and exchange information about new technologies, new threats, products, vulnerabilities, etc.

- Providing advice and guidance to Information Governance and users where applicable on:

    - Policy Compliance
    - Incident Investigation
    - Security Awareness
    - Security Training
    - Systems Accreditation
    - Security of External Service Provision

8.8 Staff Responsibilities:

All staff members are responsible for reading and co-operating with the contents of this Policy as part of their normal duties and responsibilities. They are responsible for ensuring that they maintain up to date awareness of Information & Cyber Security practices with regard to their own and their staff roles and responsibilities. This includes the responsibility to report information security incidents as soon as they occur.

9. ABBREVIATIONS / DEFINITION OF TERMS USED

ABBREVIATION	DEFINITION
AUP	Acceptable Use Policy
CD	Compact Disc
DVD	Digital Versatile Disk
ISP	Internet Service Provider
PDA	Personal Digital Assistant
PID	Personal Identifiable Data
PIN	Personal Identification Number

[1] Such as the NHS Digital CareCERT Information sharing Portal - https://nww.carecertisp.digital.nhs.uk/display/CC/CareCERT+Information+Sharing+Portal+Home

ABBREVIATION	DEFINITION
SIRO	Senior Information Risk Owner
USB	Universal Serial Bus
VPN	Virtual Private Network

TERM USED	DEFINITION
Business Vital Records	Records, regardless of medium, which are essential to the organisation in order to continue with its business-crucial functions.
Data	Individual pieces of information
Data devices	This includes any device that can store information required for the organisation's operational business. Typically this can be desktop computers, laptops, palmtops, tablets, smart phones or Personal Digital Assistants (PDAs); but also includes audio and visual recording/playback devices (such as Dictaphones, digital or film cameras, MP3 players)
Jail breaking	Removal of security controls placed on the mobile device by the vendor, thereby enabling downloading otherwise disabled.
Malware	Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system.
Media	Any physical item that can store information and requires another device to access it. For example, CD, DVD, Floppy disc, tape, digital storage device (flash memory cards, USB disc keys, portable hard drives)
Personally Identifiable Data (PID)	Personally Identifiable Data or PID is used to describe the data item(s) that could be used to identify an individual in a set of data. This could be one piece of data, for example a person's name, or a collection of information such as name, address, and date of birth. In the context of this policy this acronym equally applies to Patient Identifiable Data as defined in Section 251 of the NHS Act 2006
Teleworking / Offsite working	The situation where any member of staff works either at home or at any other site location that is not considered their office base. Although it mainly refers to staff who regularly work away from base, the main principles will also apply to a member of staff who spends the occasional afternoon working from home, or who takes work home in evenings 'to finish something off'.

DOCUMENT CONTROL

Equality Impact Assessment Date	
Sub-Committee & Approval Date	Joint IG Board 15/03/2019

History of previous published versions of this document:

Version	Ratified Date	Review Date	Date Published
NCUH IG21 Off-site Use and Security of Portable Computing v4.0	1/2/2016	Jan 2019	9/2/2016
CPFT Mobile Computing POL/077/004 VFeb16	10/2/2016	Mar 2019	Feb 2018

Statement of changes made from previous version

Version	Date	Section & Description of change
0.1 Draft	02/05/2018	• Moved both previous Trust policies into new joint template • Added policy content from both Trusts' previous policies
0.2 Draft	21/11/2018	• Amended content to remove references to specific, branded VPN and Access Control technologies.
0.2 Draft	25/01/2019	• Stakeholder amendments added for typos and syntax where applicable
0.3 draft	12/3/2019	• Reference to previous trust policies in Doc Control section
0.4 draft	19/03/2019	• Addition of separate SIRO responsibilities Section 8.3
0.5 draft	19/03/2019	**Amended following Policy Management Group meeting:** • Added Joint IG Board approval date to Policy front page and document control section, and Policy Checklist • Section 8.5 Joint IG Board Responsibilities added clarification that this is the approving committee for the Policy. • Section 8.3 Removed Associate Medical Director and left as Caldicott Guardian • Added SIRO responsibilities
1.0	28/05/2019	• Amendment to first paragraph section 3.5

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Michael Smillie	Executive Director of Finance & Strategy (Joint Director of IM&T and Estates)/Senior Information Risk Owner	10/01/2019
Robin Andrews	Interim Executive Director of Finance	10/01/2019

Name	Job Title	Date
Andrew Brittlebank	Medical Director	10/01/2019
Graham Putnam	Associate Medical Director/Chief Clinical Information Officer	10/01/2019
Dave Dagnan	Consultant Clinical Psychologist	10/01/2019
Farouq Din	Associate Director of Digital Health	10/01/2019
Daniel Scheffer	Associate Director for Corporate Governance/Company Secretary	10/01/2019
Lesley Paterson	Associate Director of Quality & Nursing (Specialist Services)	10/01/2019
Lyn Moore	Associate Director of Operations	10/01/2019
Mandy Annis	Employment Services Bureau Manager	10/01/2019
Julie Thompson	Head of Workforce Services	10/01/2019
Elizabeth Klein	Head of Nursing - Clinical Standards	10/01/2019
Jacky Stockdale	Joint Business Manager - Corporate Services	10/01/2019
Paula McBride	Deputy Business Manager	10/01/2019
Kirsty Jay	Deputy Business Manager	10/01/2019
Laura Parkinson	Head of PMO	10/01/2019
Yvonne Salkeld	Head of IG	10/01/2019
Steve Johnstone	Joint Interim Head of IT	10/01/2019
Sarah Sproat	Clinical Nurse Specialist in Palliative Care	10/01/2019
Lorraine Gray	Head of Information	10/01/2019
Natalie Karam	Head of Performance	10/01/2019
David Franklin	Financial Systems Manager	10/01/2019
Kath Watts	Network Manager - First Step	10/01/2019
Katherine McGleenan	Clinical Quality Manager	10/01/2019
Anne Gadsden	Information Governance Officer	10/01/2019
Paul Corrie	Information Governance Compliance Manager	10/01/2019
All NCUH Business Managers		10/01/2019