Use of ICB Mobile Devices (including Computers, Phones and own devices) Policy

Job Title of Policy Author	Governance Manager/IG Operational Lead
Review/Development Body	Audit Committee
Ratification Body	ICB Board
Date of Ratification/Effective from	TBC
Review Date	Three years from the date of ratification
Document Reference Number *(supplied by Governance Team)*	CG-P-011
Target audience	All ICB staff, including non-executive members, temporary staff and contractors

Contents

CONSULTATION SCHEDULE	
Title of Individual	**Groups consulted**
Jot Bougan – Health Informatics (HIS)	Shropshire & Staffordshire HIS
Granville Thelwell – EDI Business Partner	
SEG	All Staff
IG Group	

IMPACT ASSESSMENTS		
	Date Completed	**Comments**
Equality Impact Assessment (EIA)	14/02/2024	Assessment completed
Quality Impact Assessment (QIA)		(*for no impact insert: No impact identified)* *(If non-applicable insert N/A)*
Data Protection Impact Assessment (DPIA)		(*for no impact insert: No impact identified)* *(If non-applicable insert N/A)*

VERSION CONTROL				
Version	**Job Title of Lead/Policy Author**	**Ratification Date**	**Ratification Body**	**Summary of Amendments**
i.e. 1.0 (minor amendments should be 1.1, 1.2 etc)				**(only to be completed for minor amendments - for full review state 'Full review')**
1.1	Governance Manager/IG Operational Lead	TBC	ICB Board	

Document Status*: This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.*

1.0 Introduction

1.1 Mobile devices provide many benefits to an agile workforce; however, they also lead to new risks associated with the information stored on the equipment and working outside of the organisation's premises.

1.2 This policy will address the security issues and give clear instructions and guidance on the allocation and use of ICB provided mobile devices.

1.3 The organisation will aim to:

- Raise awareness among employees about cyberbullying.
- Provide a safe work environment in which preventative measures are in place to prevent cyberbullying.
- Ensure systems are in place to deal with cyberbullying should it occur.

2.0 Purpose

2.1 The purpose of the policy is to set out the responsibilities of the ICB and provide managers and employees with clear guidelines regarding the appropriate use of authorised mobile devices provided by the ICB.

2.2 The policy also covers the use of personal devices and to establish guidelines for ICB employees who wish to use their personal devices for work-related activities, and to ensure that ICB data remains secure while allowing for greater convenience and flexibility. A Personal device is defined as a device owned and procured by an individual, with the capacity to process, store or transmit information independently.

3.0 Scope

3.1 This policy applies to all employees, contractors and other individuals working for or on behalf of Staffordshire and Stoke-on-Trent ICB (including contractors, temporary staff and secondees). All staff must follow the policies agreed by the ICB.

3.2 The terms and conditions contained within this policy remain in force twenty-four hours a day, seven days per week.

3.3 The policy is based on the following principles:

- The use of mobile devices is reasonable, appropriate, lawful and in accordance with ICB requirements.
- Staff are aware and comply with this policy.
- Mobile devices provided by the ICB remain the property of the ICB; and individuals are responsible for the care and security of any mobile devices issued to them.
- This policy is mandatory, and non-compliance may result in disciplinary action up to and including dismissal and notification to the appropriate authorities of criminal or suspected criminal actions.

4.0 Definitions

Mobile device	A mobile device is a small hand-held device that has a display screen with touch input and/or a QWERTY keyboard and may provide users with telephony capabilities, including but not limited to; • Laptop/notebook computers

	• Tablet computers/iPads, • Handheld computers • Smartphones/Smartwatches • Mobile phones • Digital cameras • Digital voice recorders
Mobile Phone	A portable device for connecting to a telecommunications network to transmit and receive voice, video, or other data
Smart Phone	A smartphone is a cellular telephone with an integrated computer and other features not originally associated with telephones, such as an operating system (OS), web browsing and the ability to run software application.
Handsfree	Equipment, most commonly a phone, designed to be used without being used in your hand.
SSHIS	Shropshire & Staffordshire Health Informatics Service
SOP	Standard Operating Procedure

5.0 Duties and Responsibilities

5.1 *Chief Executive Officer*

The Chief Executive Officer has overall responsibility for maintaining an overview of the governance processes associated with this policy. Responsibility is delegated to Directors, Line Managers and all staff.

5.1.1 *Directors*

Authorisation of the purchase /rental and issue of mobile telephones and other mobile devices to all staff.

5.1.2 *Line Managers*

- Monitor compliance with the agreed procedures within their areas.
- Ensuring employee's report any loss or misuse of an ICB mobile device.
- Responsible for ensuring that all ICB property, including mobile phones allocated to their staff are returned to the SSHIS on their leaving the organisation.

5.1.3 All *Staff*

- Must be aware of the policy and their duty of care to others. To ensure that all personal information must be treated carefully and must not be disclosed to unauthorised persons which is line with the confidentiality clause of their contract of employment.
- Must take particular care when working at home or in a public place to ensure that their screen is not overlooked, or conversation overheard.
- Must use authorised mobile communication devices responsibly, lawfully and in accordance with the terms of this policy and comply with the ICB Social Media Policy at all times.
- Must take all reasonable steps to maintain the security of the equipment issued to them i.e. not leave devices unattended or left overnight in a car etc
- Must ensure that antivirus updates are installed on a regular basis.
- Must report any breaches of the policy (abuse, loss, theft) so that steps can be taken to secure data (for example, remote wipe).
- Must report all cases of suspected fraudulent usage of mobile communication devices to the ICB's Fraud Champion and/or Local Counter Fraud Specialist.

- Must return their mobile communication device(s) to their manager, when leaving the ICB.
- **Must not use ICB Issued mobile devices for personal use except for use in the event of an emergency.**

6.0 Acceptable Use of Mobile Devices

6.1 Acceptable Use of laptops

6.1.1 Personal use of the Internet should be limited and not impact on your job duties. Preferably such access should be limited to your own time, for example during your lunch break, or after you finish working.

6.1.2 You must not create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.

6.1.3 Unsuitable material might also include data, images, audio files or video files the creation, publication or transmission of which is illegal under British law, and material which is against the rules, essence and spirit of this and other policies.

6.1.4 Users must not enter or utilise real time chat facilities or enter or use online gaming or betting sites.

6.1.5 You should not enter your work email address on a website except for work purposes.

6.1.6 The above list gives examples of some “unsuitable” usage but is neither exclusive nor exhaustive. If you are in any doubt about any particular material or activity, you should check with your manager.

6.1.7 Annual leave plays a vital role in supporting employee wellbeing, productivity, and work-life balance by ensuring time is allocated for rest and recuperation. Staff are strongly encouraged **not** to take **work laptops, phones, or undertake work-related tasks during their holidays,** as this detracts from the intended benefits of leave. Unless required for work purposes, employees should leave work equipment at home to maximise their break. If it is necessary to use work devices—for example, during a "workation"—staff must first confirm compliance with company policy and insurance guidelines.

6.1.8 For both domestic and international travel, formal agreement and documentation **must** be **obtained in advance** from your **Line Manager**, with technical feasibility confirmed through the Health Informatics Service (via a Service Desk ticket). While it may be technically possible to arrange such access, approval is subject to specific exemptions and circumstances. Explicit authorisation from your Line Manager, documented by email, is required for audit purposes.

6.1.9 Prior to travel, employees **must review** ICB and SSHIS IG-IT data security, data protection, and networking policies, and arrange a secure VPN via the Health Informatics Service. Consider all relevant legal and country-specific data import/export restrictions, including those concerning encrypted ICB devices, as advised by the Foreign travel advice - GOV.UK service.

6.1.10 If using personal or “Bring Your Own Device” (BYOD) equipment, it may only be used for O365 connections to ICB Teams meetings and must not be used to access the corporate network. IT-IG security and insurance liability for personal devices remain solely with the employee; ICB coverage does not extend to personal equipment. Even

when only personal devices are taken abroad, prior approval from SSHIS is required, as this may trigger security alerts or breach data protection regulations.

6.1.11 To mitigate IT and cyber security risks, always use a secure VPN, ensure full disk encryption is enabled, and keep all ICB software up to date. Avoid using public Wi-Fi networks unless appropriate protections are in place.

6.1.12 International travel may subject your laptop to customs or security inspections, and certain countries impose strict regulations on technology, data, and encrypted devices. Some destinations prohibit the entry of devices entirely (refer to Foreign, Commonwealth & Development Office advice for areas that UK citizens should not travel to). Devices should be carried in hand luggage to minimise the risk of loss or damage.

6.2 Software

6.2.1 All software SHOULD be procured through the S&SHIS procurement team.

6.2.2 You SHOULD NOT install any software or application on S&SHIS computer equipment unless you are authorised to do so, and a valid license exists for the software or application.

6.2.3 Personal or unsolicited software SHOULD never be installed on S&SHIS computer equipment.

6.3 Allocation of Mobile Phones

The ICB has set the following criteria for staff to be issued with a mobile phone:

- The employee is on call or needs to be contactable outside of normal working hours for business continuity e.g., Silver and gold on call, Executive team, EPRR, Urgent and Emergency Care.
- The employee's duties require them to occasionally spend time out of the office – e.g., Safeguarding, (any other clinical areas).
- Corporate services support staff who manage the reception calls and rota – Band 3 admin assistants who regularly attend the offices - all other staff on the rota have a direct Teams line.
- Employees who have regular contact with external organisations as part of their day-to-day role. To include complaints team and governance team who have contact with patients, solicitors etc and CSU contacts.

6.4 Use of Mobile Devices

It is important that the ICB demonstrates value for money in the use of its mobile devices. Staff issued with mobile smartphones with data capabilities should be mindful of usage allowances and keep work related web browsing to a minimum.

The device should not be used for personal or non-work-related web browsing.

Wherever possible contact will be made through Teams or use of a landline.

Staff are expected to connect devices to Wi-Fi wherever possible. If staff are tethering (in the context of mobile phones, this refers to allowing another device to use the data connectivity of the mobile phone) please keep in mind that utilising the data connectivity in this way is expensive for the ICB.

When not in use Wireless and Bluetooth connectivity should be turned off.

It is the employee's responsibility to keep the mobile communication devices charged and ready for use and authorised mobile communication devices need to be switched on when the member of staff is on duty or on call.

Users must respond to device software updates that are communicated via SSHIS in a timely manner to ensure that its operating system is up to date.

6.5 Personal calls/usage

All mobile devices are provided by the ICB for ICB work related purposes except for use in the event of an emergency.

The mobile device always remains the property of the ICB.

All devices must be returned to the SSHIS when an employee leaves the organisation. Failure to return any devices is considered as theft and the Police will be informed. A ticket should be logged via SSHIS Service Desk confirming the date when the device(s) will be returned.

6.6 Voicemail

Voicemail messages should be set up on the phone indicating name and their role in the ICB.

6.7 Videos, images and voice recordings

Taking of images, video or recordings containing individuals is only allowed when the subjects have given specific consent.

Mobile devices should only be used for recording meetings in accordance with the SOP for Effective Teams Meetings. Any recordings should only take place with the express permission of those present at the time of the recording.

6.8 International Calls

As standard, all International/Premium Rates Services are barred on all ICB devices.

6.9 Installation of Apps

Your phone will have been pre-loaded with software applications (Apps) such as a Outlook, calculator etc. If you require additional Apps to perform your work duties, please contact the SSHIS who will advise on suitability and security of the App. Please inform your line manager if you need to use additional Apps.

6.10 a) Security

Each mobile device shall be configured by SSHIS in accordance with defined standards, that are appropriate to its use and takes account of NHS requirements, standards, recommendations, and guidelines for such devices.

Devices which are used to store personal confidential information of patients or staff for example in the form of voice mail, email, or text messages, must have strong passwords set on the device. These will also be subject to controlled onward use and secure disposal. Failure to ensure that security measures are in place on a device used for work purposes, could be treated as misconduct or as gross misconduct leading to disciplinary procedures up to and including dismissal.

b) Security Measures

- ICB supplied devices which are synchronised to accept your emails, have enforced security including passwords, protection against data storage in the cloud, and remote wipe facility in case of loss or theft.

- Any ICB supplied smartphones that are not linked to synchronised emails and do not have enforced security must be reported to the SSHIS service desk immediately in order that action can be taken to rectify this.
- Users shall comply with ICB policies and NHS best practice guidance concerning the requirement for access to information; that information should be shared only on a 'need to know' basis. Storage of sensitive information on ICB equipment shall be kept to the necessary minimum (in respect to both content and duration).
- SSHIS will notify the current network providers where necessary. Report any breaches of the policy (abuse, loss, or theft) to the Governance team, quoting the SSHIS service desk reference and police crime number where appropriate.
- The employee is responsible for taking reasonable precautions to avoid loss or misuse of their mobile communication device. This includes not leaving it in view in unattended vehicles and storing it securely when not in use.
- Any materials for personal use applications or ringtones are not permitted, as viruses can often be embedded in these materials, thereby rendering the mobile device inoperable.
- Personal Cloud Storage must not be used in any circumstances.

6.11 Confidentiality

Staff must refer to the principles of the Data Protection Act and Caldicott Principles to ensure that mobile devices are only used to discuss personal, sensitive, or confidential issues in circumstances that are otherwise unavoidable. If another more secure method is available, then staff should be using that method.

Texting, WhatsApp and Messenger, etc are not a safe method of transmitting patient identifiable, sensitive or confidential information. If it is necessary to refer to a patient/service user or staff member, the message should avoid identifying any individual. This can be achieved by, for example, using just initials and being careful not to include any additional information such as an address or post code that might identify them. If including personal identifiable information in a message cannot be avoided, then that individual's consent must be obtained in advance.

6.12 Cyber Bullying

The ICB does not and will not, tolerate any member of its staff being bullied or harassed and any incidents should of such behaviour should be reported to your line manager, HR or Freedom to Speak Up Guardians. Provide a copy of the harassment /bullying correspondence from whichever platform it occurs on, for the file and continue to report any further episode that may occur. This policy relates to remote working as well as the use of social media channels.

Behaviours that make someone feel intimidated or offended could be constituted as bullying or harassment. It will often involve someone sending, posting or sharing negative, offensive, harmful, false or humiliating material about someone, or otherwise acting in a manner to them which is intentionally mean or intimidating. Examples include:

- Threatening another person
- Embarrassing another person
- Aggressive and/or rude texts, tweets, posts or messages
- Inappropriate pictures or videos designed to hurt or embarrass a person
- Posting personal information
- Spreading malicious rumours
- Unfair treatment
- Picking on or regularly undermining someone

- Not promoting them for spurious reasons

However, cyber bullying can be far less explicit. It may take the form of an unnecessary or ambiguous comment or post; for instance, saying to a colleague "I'm still waiting for X to complete the project…"

This could insinuate that person X is at fault, even though the speaker knows that person X has been off work sick and will be completing the project later that day.

Cyber bullying can also include sharing personal or private information, sharing photos with a view to causing embarrassment or humiliation, as well as hacking someone's account or tricking them into sharing personal information. Alternatively, the bullying may be by way of deliberately leaving someone out.

Where possible you should block the account that the bullying/harassment is received from.

6.13 *What should you do if you are subject to cyberbullying?*

Report it immediately to your line manager, director, Freedom to Speak Up Guardian, Mental Health First Aider, HR or any other person you trust. If you do not feel that you are able to raise this yourself, you can ask for support and it being raised on your behalf, it should be noted that confidentiality will be difficult to maintain in order to achieve a resolution/outcome.

6.14 If the bullying is occurring on your personal social media, report it to the platform holder, block the perpetrator, if the bullying includes any threats of death, violence or stalking, consider reporting it to the police. Make your manager aware of the threats.

6.15 Also refer to the ICB's Bullying and Harassment Policy which is available on IAN.

6.16 Any member of the ICB's staff found to be carrying out acts of bullying or cyberbullying will face disciplinary action; as referred to in the Disciplinary Policy, which is available on IAN.

7.0 Safety

7.1 The Management of Health and Safety at Work Regulations 1999 require the ICB to ensure sufficient information and instruction is provided to confirm the appropriate Health and Safety Legislation and associated Regulations. It is an offence to use a hand-held phone when driving, which incurs a fixed penalty notice. Should a fixed penalty notice be incurred, this penalty charge will not be reimbursed by the ICB.

7.2 The ICB reserves the right to consider disciplinary action if it is brought to our attention that an offence has occurred whilst using ICB equipment.

7.3 Use of a handsfree mobile phone when driving is not illegal, but the ICB strongly advises against its use as it can reduce concentration on driving and is associated with a higher incidence of accidents. Mobiles should be set to go to voicemail whilst driving.

8.0 Incident reporting

8.1 Damage to a mobile device

Recipients of ICB mobile devices are responsible for their care. Recipients must report any defects or damage as soon as reasonably practicable to their line manager and the SSHIS. Recipients losing or damaging an ICB mobile device where they are

deemed not to have taken appropriate care of it will be required to pay in full or in part for a replacement.

8.2 In the event of a lost or stolen device, the employee must report the incident immediately to both the ICB and the Health Informatic Service (HIS):

During the working day 9am-5pm	Outside working hours
• Service Management Tool Portal; https//smt.sshis.nhs.uk/ • Phone; 0300 303 1673 governance@staffsstoke.icb.nhs.uk	Contact the local police immediately Governance team next working day

8.3 The HIS reserves the right to remotely wipe corporate data to prevent unauthorised access. Remote wipe will include corporate data only and has no access to personal data on the device. Users should also seek guidance from the manufacturer for remotely wiping personal data.

Employees should ensure that the Governance Team is notified immediately of any loss of damage, delays in reporting incur significant costs or the organisation and which may be passed on to the registered user of the device.

9.0 Use of Personal Devices

9.1 This policy sets out the guidelines for staff who wish to use their personal devices for work-related activities and to ensure data remains secure while allowing for greater convenience and flexibility.

9.2 *Acceptable Use*

Employees are permitted to access ICB data and resources from their personal devices for work purposes only. Personal device usage that interferes with normal work duties is prohibited, such as the use of social networking (i.e. Facebook, TikTok) video blogging (i.e. YouTube), microblogs (Twitter), blogs etc during work time.

9.3 Enrolled BYOD devices will not be granted access to the S&SHIS managed corporate network. Corporate data can only be saved in managed apps locally on the device such as OneDrive for Business, anything outside of managed apps is outside of this BYOD policy.

9.4 The user shall take reasonable steps to:

- Prevent theft and loss of device i.e., not leave them unattended.
- Keep information confidential where appropriate, including from friends and family who may have access to the device.
- Devices that are shared, such as with other family members, cannot be used as a BYOD as there is increased risk of information leakage.
- Remove data from the device before it is disposed of, sold, or transferred to a third-party or at the end of employment.

9.5 *Security*

Employees must comply with all existing security policies. Where available, devices should have up-to-date antivirus, malware protection software and should have the latest software versions/security patches installed (as advised by software/device manufacturer).

9.6 The following settings will be applied automatically by the HIS at device enrolment in accordance with the Microsoft Centre for Internet Security which is subject to continual review and improvement. Settings below are subject to availability on the relevant operation system (OS); once applied to the device, the Device Management Policy can be viewed on the device itself.

- Pin and password security
  - Ensure mobile devices require the use of a password.
  - Password reuse is prohibited, and expiration of compliant passwords will not be set to expire.
  - Minimum password and pin length will be required: 8 characters.
  - The use of simple pin and passwords will be prohibited.

- Device hardware settings
  - Devices will automatically lock after a period of in activity: 5 Minutes.
  - Devices will be set to wipe on multiple sign-in failures to prevent brute force access.: Max of 10 failed logins this will wipe corporate data only and will not affect personal data.
  - Device encryption will be enabled.
  - Access from rooted or jailbroken devices will be blocked.

- Applications
  - The Microsoft Company Portal, and Microsoft Authenticator app will be required to facilitate the enrolment of mobile devices.
  - Restrictions on the applications when accessing trust data will be applied including but not limited to:
    - ✓ Block copy and paste.
    - ✓ Block print
    - ✓ Block saving trust data to the local device other than managed applications.
    - ✓ Block backup of trust data within an application to OS native backup solutions.

10.0 Privacy

S&SHIS respects the privacy of employees. However, in cases where S&SHIS needs to protect corporate data, S&SHIS reserves the right to remove corporate data and work profiles from any device enrolled without notice. Corporate data held on devices is subject to the Freedom of Information Act and the provisions of the Data Protection Act 2018.

What S&SHIS can see and cannot see on your device is displayed at enrolment time, from within Company Portal once enrolled and on the Microsoft site: https://learn.microsoft.com/en-us/mem/intune/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune.

As of 22/09/23 this is as follows:

11.0 Device Support

11.1 While the S&SHIS will provide guidance on setting up access to the data and resources, it will not provide full technical support for personal devices.

12.0 Training and Implementation

12.1 There are no specific training requirements associated with this policy. However, when issuing a ICB mobile device, the Issuing Department or line manager will ensure the recipient is aware of their duties and responsibilities under this policy.

Any employee who has queries regarding the content of this policy or has difficulty understanding how this policy relates to their role, should contact the Governance Team.

Failure to comply with this policy will result in your access from BYOD being revoked. The ICB-ICS IG Data and Digital Committee is responsible for monitoring compliance and the effectiveness of this policy through the reporting of incidents as required.

13.0 Review, Ratification and Archiving

13.1 Policy has been developed following a review of other NHS organisational Mobile Devices policies and in consultation with the SSHIS, Human Resources Directorate and Staff Engagement Group.

The policy will be reviewed every three years or sooner if national policy/guidance changes.

14.0 Dissemination and Publication

Dissemination of the final policy is the responsibility of the author. They must ensure the policy is uploaded on the intranet via the Communications Team. The Communications team is responsible to issue an organisation-wide notification of the existence of the Policy.

Heads of Departments/Managers are responsible for ensuring that all staff (including bank, agency, contracted and volunteers) have access to and are made aware of policies that apply to them.

All staff will be able to access copies of policies via the policy section of the ICB intranet

15.0 References and Associated Documents

ICB Policies consulted:

- Disciplinary Policies
- Bullying and Harassment Policy

SSHIS Policies consulted:

- B4c SSHIS Elevated User Rights Policy
- C1a & C1c SSHIS Infrastructure Logging and Event Management Procedure
- B3e SSHIS Secure Device Disposal Procedure
- B4d SSHIS Vulnerability Management Policy
- 9.1.1 SSHIS Network Security Policy

See also:

- National Cyber Security Centre – Device Security guidance Device security guidance - NCSC.GOV.UK
- Gov.UK – Smart devices : using them safely in your home Smart devices: using them safely in your home - GOV.UK

16.0 Impact Assessments

16.1 *Equality Impact Assessments are carried out to demonstrate due regard to (1) the public sector equality duty (PSED) 3 aims, dropping down from the Equality Act 2010 to: eliminate discrimination, harassment victimisation; advance equality of opportunity; and foster good relations", (2) The Health & Social Care Act 2012 re evidencing showing due regard to reducing health inequalities between the people of England."*

Initial Assessment Statement

'This policy has been through an Initial Assessment process and no identifiable or potential adverse impact against any protected characteristics or inclusion health group have been identified or mitigating actions have been taken. In the event of any new data, information or reporting, identifying any adverse or potential adverse impact, this assessment will be reviewed, and a full impact assessment will be carried out where it is deemed necessary to do so. Accessible and inclusive Information and equality monitoring (where it is practical to do so) have been considered.'