NICS Mobile Device Security Policy

Version: 1.4

Status: Published

TRIM Reference: FI1/18/858845

Author: Central IA Team

Date: August 2018

Table of Contents

1. DOCUMENT HISTORY

Version	Date	Author	Changes
0.1	July 2012		Initial update of existing Laptop Policy & PED Policy documents
0.2	Aug 2012		Merge and edit of Laptop Policy & PED Policy documents
0.3	Aug 2012		Update to reflect initial IA Team QA
0.4	Sept 2012		Update for QA by EDA and ITSOs
0.5	Oct 2012		Update for QA by NICS Accreditation Panel and SIRO Forum
1.0	Feb 2013		Approved for issue
1.1	Feb 2014		Updated to reflect changes to information classifications with effect from 2 April 2014
1.2	April 2016		Updated to reflect removal of Ironkeys
1.3	Dec 2016		This policy incorporates the NICS Mobile Device Policy and replaces the NICS Laptop and Mobile Device Security Policy.
1.4	Aug 2018		Adjustments to reflect the establishment of NCSC, GCS and GDPR.

1.1. DOCUMENT STAKEHOLDER LIST

Name	Date
Central IA Team	September 2012
ESS EDA EDT	September 2012
NICS ITSO Forum	September 2012
NICS Accreditation Panel	November 2012
NICS SIRO Forum	December 2012
Protective Marking Sub Group	February 2014
NICS ITSO Forum	June 2016

IGIB	December 2016
Central IA team	August 2018

2. INTRODUCTION

This policy applies to all NICS approved and supported mobile devices.

For the purposes of this document, the term 'mobile device' includes, but is not restricted to, IT Assist supplied and supported laptops, mobile phones, smartphones, tablets and approved external storage devices which can be used to access, store, process, transmit, discuss, or record data electronically.

This security policy provides the reasoning and processes for minimising the risk associated with handling (accessing, storing, processing, transmitting, discussing or recording) Official information on mobile devices. Its purpose is to ensure that staff[1] members are fully aware of the security required to protect assets, in particular sensitive or personal information, and should be read in conjunction with the NICS Use of Electronic Communications Policy.

At all times users must also comply with their own departmental policies and overall NICS policies.

The loss of a mobile device and the subsequent loss of government data are considered to be a security compromise. In addition to the laptop/mobile device and its data being unavailable for business use, there is also the potential for disclosure of Official information. Such a loss of information will often be deemed more serious than the loss of the physical asset. A disclosure of information, especially if it is personal or sensitive may lead to a disruption to business continuity because of the work required to mitigate/explain the loss. However, the NICS may also fail to meet statutory obligations and it could potentially incur fines of up to £500k by the Information Commissioner Office (ICO). This could result in both financial and reputational damage to the NICS.

Within the NICS, the Corporately Owned Personally Enabled (COPE) initiative has been introduced. It is a recognition that, while a device is provided primarily for work use, in order to support initiatives such as work life balance, an element of personal use is permitted. In using the device for personal purposes staff recognise and accept that they must not use the device for any inappropriate purpose or anything which would contravene departmental or NICS policy. Any breach of policy shall be viewed as a security incident and dealt with as such, possibly leading to disciplinary action.

Further guidance on the use of COPE Devices is detailed here COPE Devices Guidance

[1] **This policy applies to everyone who accesses NICS systems, networks or computers; regardless of whether or not they are directly employed by the NICS.**

3. PERSONAL RESPONSIBILITIES

- Users are responsible for the physical security of all mobile devices provided for work purposes, AND for the information stored on them**.**
- The mobile device remains the property of the NICS and must only be used in accordance with official guidelines.
- **All incidents or breaches of security, including any lost mobile devices must be reported immediately** or as soon as reasonably possible to IT Assist I&S if inside network or I&S if external to the network, email **itassist@nigov.net**) Where a crime is suspected, contact PSNI.
- Staff should note that, as is permitted by legislation, all activity is logged and monitored and they should have no expectation of privacy whether the purpose is for official business or personal use.
- At the NICS's request, users shall deliver the mobile device to IT Assist if and when the device is selected for a physical security audit or is needed for e-discovery purposes
- Authentication credentials such as **tokens, passwords or other items necessary to access the information must not be stored with the mobile device at any time.**
- Where large quantities of data (for example greater than 1,000 records), or any sensitive/personal data, is held on a mobile device, risk assessments **must** consider the full impact of loss or compromise of the data. **(NB**: **Storage of any personal or sensitive information, even on a temporary basis, must be approved by the Information Asset Owner (IAO). A Privacy Impact Assessment (PIA) should be completed within the business area).** It is also important to remember that data in deleted files must be assumed to persist including on smartphones. Therefore devices must be sanitised securely in line with **https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media**
- The transfer or storage of data is only permitted on approved devices using approved methods. Speak to your Departmental IT Security Officer (ITSO) or Departmental Information Manager (DIM) for further advice.
- Information classified as higher than Official should not be entered or stored on any mobile device.
- Staff must ensure that their mobile device is not used by anyone else.
- Users are not authorised to change the system configuration or the hardware profile.
- Mobile devices for the purposes of training or presentations are allocated to an individual member of staff who is responsible for ensuring that appropriate security controls are in

place e.g. sign-in/sign-out procedures. Sensitive/personal data must not be held on these devices.

- The use of devices that are “jailbroken”, "rooted" or have been subjected to any other method of changing built-in protections is not permitted and constitutes a material breach of this policy.
- Where a mobile device is no longer required by its original recipient, it must be returned to IT Assist for secure erasure, reloading of software, re-encryption and redeployment. It must not be retained by the Branch as a spare.
- In exceptional circumstances there may be a requirement for a mobile device to be reallocated to another member of staff within a Branch. In this case, prior written approval from a Grade 5 is required and it is the responsibility of the Head of Branch to ensure that appropriate training has been provided in the use of the mobile device. It is also their responsibility to ensure that this is recorded in an auditable, business process and that IT Assist are informed.
- IT Assist may monitor the use of mobile devices for purposes of security and administration.
- Bluetooth should be switched off when not in use. Users should be aware of HR Policy and safety advice concerning hands free operation.

3.1. PERSONAL RESPONSIBILITIES – LAPTOP SPECIFIC

- Users requiring a laptop to replace their desktop PC need Grade 5 approval.
- On receipt of a laptop, the user is required to sign the declaration issued by IT Assist accepting that they will comply with this policy and acknowledging that they are responsible for the physical security of the laptop as well as the information stored on it.
- Users must ensure that their laptop is secured with a cable lock during office hours.
- Sleep mode has been disabled on all laptops. A user who intends to leave a cable-locked laptop within their secure workplace for a temporary period must ensure that it is left in ‘locked’ mode.
- Laptops must be properly closed down at the end of the day (i.e. selecting shutdown from the operating system menu) and secured in a suitable locked cabinet[2] within the place of work.

Note – Cable locks are not secure out of office hours.

- Only approved, external media products are to be connected to the laptop.

4. DATA STORAGE / TRANSFER

[2] For further guidance on the suitability of office furniture contact your ADSO.

- IAOs in business areas with a requirement to transfer a large volume of data should use the ITAssist accredited SFTP service.
- IAOs in business areas with a requirement to store or transport a large volume of data must ensure that the devices used are appropriately encrypted.
- Approved devices required for data storage are available from IT Assist through the IT Assist Service Request Procedure.

5. OTHER DEVICES

Only NICS devices may be connected to your NICS laptop/PC. If the device required is not available in the IT Assist catalogue, discuss the requirement with the business owner and your Departmental ITSO and seek approval from your Grade 5.

5.1. DIGITAL CAMERAS

- Only digital cameras that have been provided and approved (by your Grade 5) for read-only business use can be connected to your work laptop or desktop PC. Where there is difficulty accessing the digital camera from a laptop or desktop, users must contact IT Assist who will endeavour to resolve the issue.

5.2. MULTI-MEDIA DATA CARDS/MEMORY CARDS (E.G. SD, COMPACT FLASH)

- Multi-Media Data Cards must not be used to transfer or store NICS information. Where there is a need to transfer or undertake short-term storage of information then an approved method of transfer must be used [See Section 4].

6. COSTINGS

- Users shall NOT authorise any purchase or service from their mobile devices which may be chargeable to their mobile phone account, e.g. car parking. or apps.
- The user’s business area shall retain responsibility for the approval and payment of out-of-warranty repairs.
- Users shall be liable for costs incurred in relation to personal voice and data connections outside of agreed tariff allowance.

7. WIFI CONNECTIVITY

The NICS has invested in a wireless infrastructure to enable corporate devices to connect via wifi networks. More information can be found here Wireless Connectivity

8. TRAVELLING ABROAD

Mobile devices including laptops **MUST ONLY** be taken outside the EU when there is a business requirement and written approval from the Grade 5.

- If travelling or working overseas, contact your ADSO or Departmental ITSO to check whether additional security restrictions apply.
- The Departmental ITSO and IT Assist must be informed.

9. ASSET MANAGEMENT

- All devices must be recorded on an Assets Register and managed in accordance with the guidance in ‘Guidance on Security of Portable Assets’.
- When a staff member leaves a business area on transfer or exit, the asset record should be updated in the appropriate assets register.
- The device shall be set up and registered with corporate email addresses and these shall not be modified. The OS must be used "as is" with the device functionality not being modified by the user, unless required or recommended by NICS.
- At end of use, all devices must be returned to IT Assist for reallocation or secure disposal

10. PASSWORD MANAGEMENT

- You must never disclose your password/pin to anyone (including IT Support staff, your manager or a colleague).
- It is acceptable to write your password/pin down, but it must be stored securely – and never with the device itself. For example, if you write your password/pin down, seal it into an envelope, and then store it according to its sensitivity (e.g. kept in a secure, locked cabinet). Under no circumstances should you ever carry this copy of the password/pin with your device.
- If you suspect that your password/PIN has been compromised you must report this to the Departmental ITSO and contact the IT Assist Helpdesk **I&S** from inside network or **I&S** from outside the network) to request an immediate password/PIN change.
- If you forget your password, contact IT Assist Helpdesk to request a reset.

11. EXEMPTIONS/EXCEPTIONS

- EXEMPTIONS FROM THIS POLICY CAN ONLY BE GRANTED IN THE MOST EXCEPTIONAL CIRCUMSTANCES AND THEN ONLY IF APPROVED IN WRITING BY A GRADE 5 IN CONSULTATION WITH THE DEPARTMENTAL SECURITY OFFICER (DSO).

THE EXCEPTION TO THIS POLICY WITHIN THE NICS ARE THOSE BUSINESS FUNCTIONS HOSTED WITHIN THE IT ASSIST CONFIDENTIAL (ITAC) NETWORK. AS A RESULT OF HAVING A CLASSIFICATION HIGHER THAN OFFICIAL, INCREASED LEVELS OF SECURITY AND ENCRYPTION ARE REQUIRED OR IN SOME CASES ASPECTS OF MOBILE FUNCTIONALITY PROHIBITED.

12. INCIDENT REPORTING

- **ALL INCIDENTS OR BREACHES OF SECURITY MUST BE REPORTED IMMEDIATELY** or as soon as reasonably possible to IT Assist I&S rom inside network or I&S if external, email **itassist@nigov.net**) who will inform the Departmental ITSO.
- An incident is defined as an issue that comes to the attention of a member of staff, which breaches Departmental policy or legislation. This includes the loss of control, compromise, unauthorised disclosure, unauthorised possession and/or unauthorised access of the Department's information, whether physical, electronic, or in spoken word or recording.
- Users should keep a record of the laptop/mobile device Badge Number and contact information needed in an emergency to report if the laptop/mobile device is lost or stolen.
- Users should attempt to power down and secure the laptop/mobile device if they have any warning that it is likely to be maliciously taken from them.
- Damage to (including suspected tampering) or loss of a laptop or other mobile device must be reported at the earliest opportunity to ITAssist, who will advise on the action that must be taken, and will inform the Departmental ITSO. The ITSO must immediately undertake a "Damage Assessment", which will include a review of the security of the laptop, mobile device and associated passwords, to determine whether security may have been comprised. As part of the damage assessment the sensitivity of the information stored must be recorded.
- The loss or theft of a mobile device must be reported to the police. The PSNI incident number should be included on the incident form.
- Users MUST connect their laptop to the network AT LEAST ONCE EVERY MONTH to ensure that security, anti-virus and other updates are deployed to their laptop as appropriate[3]. Where this has not been possible, contact IT Assist for advice.

  (This will be monitored by IT Assist and failure to comply will be identified and raised through the appropriate channels in each Department).
- For further advice and guidance refer to the IT Assist Helpdesk I&S

[3] Connection is acceptable over Secure Remote Access. However, it should be noted that downloads could be extremely slow. The recommendation is that all equipment is physically connected at a government office at least once a month.

13. ELECTRONIC DOCUMENT AND RECORD MANAGEMENT

- In line with NICS Policy, information should be stored on RecordsNI, the approved repository for NICS documents and records management. Therefore, there must be a justified business need and careful consideration before information is stored directly onto a laptop or mobile device.
- Staff are reminded that information classified as higher than Official must not be input or stored. The Departmental Information Manager (DIM) should be contacted for further guidance.

14. STAFF MOVES, RE-USE AND SECURE DISPOSAL OF DEVICES

- When a member of staff leaves an organisation or moves to a new post their line manager must contact IT Assist to arrange for the return of all NICS equipment they hold, and to ensure that email and network accounts are amended or disabled as appropriate.
- **All** mobile devices must be disposed of securely using the Secure Disposal contract (Removal, Recycling and other Disposal Services of Redundant Electrical and Electronic Equipment (Including ICT Equipment) to include Data Eradication when required).

15. POLICY REVIEW & FURTHER GUIDANCE

- This policy will be reviewed annually or in response to new legislation or regulation or following a significant security incident.
- If you encounter any operational difficulty in adhering to this policy, you should contact your Departmental ITSO in the first instance. Issues concerning the policy will be referred through your ITSO to the **Central Information Assurance Team** .
- Further Guidance, including self service training and FAQs, is also available on the **NICS Mobile Support** web page.

You should contact your Departmental ITSO if you require any further advice on any aspect of this policy.

Any breach of this policy may be viewed as a security incident and dealt with as such, possibly leading to disciplinary action.

16. GLOSSARY

Term/Abbreviation	Meaning
Accreditation	A formal, independent assessment of an ICT system or service against its IA requirements in the context of business need.
ADSO	Assistant Departmental Security Officer
COPE	Corporately Owned Personally Enabled.
DIM	Departmental Information Manager
DSO	Departmental Security Officer
EDA	Enterprise Design Authority
EDT	Enterprise Design Team
ESS	Enterprise Shared Services
Information Asset	A body of information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.
HP RM	HP Records Manager – previously TRIM System used for RecordsNI
IAO	Information Asset Owner
IT Assist	NICS ICT Services delivery partner
ITSO	IT Security Officer
NCSC	National Cyber Security Centre
NICS	NI Civil Service [All Departments, NDPBs, ALBs etc]
PSN	Public Service Network
RecordsNI	NICS Electronic Record and Document Management System
SIRO	Senior Information Risk Owner. The board level executive with particular responsibility for information risk