Commission for
Victims and Survivors

Laptop and Mobile Device Security Policy (Including Smartphones and Personal Electronic Devices)

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

1.1. 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

1.2 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
CESG	Communications-Electronic Security Group
DIM	Departmental Information Manager
DSO	Departmental Security Officer
EDA	Enterprise Design Authority
EDT	Enterprise Design Team
ESS	Enterprise Shared Services
GSi	Government Secure Intranet
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.
IAO	Information Asset Owner
Ironkeys	IT Assist issued USB approved for data transfer and storage
IT Assist	NICS ICT Services delivery partner
ITSO	IT Security Officer
NICS	NI Civil Service [All Departments, NDPBs, ALBs etc]
PSN	Public Service Network (GSi replacement)
RecordsNI	NICS Electronic Records Management System
Senior Information Risk Owner (SIRO)	The board level executive with particular responsibility for information risk
TRIM	Tower Records Information Management system used for RecordsNI

2. INTRODUCTION

This policy applies to all mobile devices.

For the purposes of this document, the term 'mobile device' includes, but is not restricted to, laptops, mobile phones, smartphones (e.g. BlackBerry), tablets (e.g. iPad, Playbooks), other Personal Electronic Devices (PEDs) and approved external storage devices which can be used to access, store, process, transmit, discuss, or record data electronically.

The purpose of this Security Policy is to ensure that staff[1] members are fully aware of the security required to protect assets, in particular government information. It has been updated to reflect the new Protective Marking Scheme which comes into effect on 2 April 2014, and should be read in conjunction with the NICS Use of Electronic Communications Policy.

At all times users must also be aware of their own departmental ICT security policies and overall NICS ICT security policies.

2.1 AUTHORITY

This Security Policy has been developed by the Central Information Assurance Team and this version approved by the Protective Marking Sub Group.

3. EXECUTIVE SUMMARY

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 personal or sensitive information. Such a loss of information will often be deemed more serious than the loss of the physical asset.

This policy provides the reasoning and processes for minimising the risk of handling (accessing, storing, processing, transmitting, discussing or recording) sensitive or personal information on laptops and all other mobile devices.

All NICS laptops used for day to day business must be encrypted using BitLocker. The approved device for temporary data storage is the Ironkey or an encrypted hard drive.

The main points to note:

- **Users are responsible for the physical security of all mobile devices provided for work purposes, AND for the information stored on them.**

[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.**

- **All incidents or breaches of security, including any lost mobile devices must be reported immediately** or as soon as reasonably possible to IT Assist (03001234155 if external to the network, email itassist@nigov.net)
- 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.
- Mobile devices need to be stored securely and/or kept close to the owner/user at all times especially in public places.
- Mobile devices must be stored in a physically secure location when not in use.
- No mobile device should be left unattended, especially when in use.
- Authentication credentials used with any disk encryption product such as **Ironkeys, tokens, passwords or other items necessary to access the information must not be stored with the mobile device at any time.**
- Users should treat all mobile devices and authentication credentials with the same care as they would their valued possessions.
- 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 on the hard disk (i.e. must be disposed of securely in line with HMG IA Standard 5).
- The information stored on any mobile device should be kept to the absolute minimum required for effective working.
- The transfer or storage of data is only permitted on Ironkeys issued through IT Assist or on encrypted hard drives, and not on any other device. IT Assist provided Ironkeys are managed centrally to facilitate password resets. Lost or stolen Ironkeys can be remotely destroyed to protect the data.
- The NICS network is accredited at IL3 level. Information classified as higher than IL3 should not be entered or stored on any mobile device.
- Any breach of this policy will be viewed as a security incident and dealt with as such, possibly leading to disciplinary action.
- Further guidance, if required, is available from the ITSO or ADSO.

4. LAPTOP AND IRONKEY PROCEDURES

- NICS laptops are encrypted with Microsoft's CESG approved BitLocker product, which uses the Ironkey USB drive for booting up the laptop and for secure data storage**. The Ironkey is the only USB storage device that can be used without IT Assist intervention. Only laptops provided and encrypted by IT Assist can be used by staff.**

4.1. SECURITY PROCEDURES FOR STAFF USING LAPTOPS

- On receipt of their laptop, the user is required to sign the declaration issued by IT Assist accepting that they will comply with the security procedures and acknowledging that they are responsible for the physical security of the laptop and Ironkey, as well as the information stored on them.
- The Ironkey must only be present in the USB port during the start-up process or when accessing/storing information on the Ironkey and must be removed and held securely at all other times.
- **The Ironkey must not be stored with the laptop at any time. Likewise Ironkeys, their passwords and BitLocker PINs must be kept separately at all times**.

4.2. PERSONAL RESPONSIBILITIES

- Users requiring a laptop to replace their desktop PC need Grade 5 approval.
- Users are responsible for the physical security of their laptop and Ironkey at all times.
- Laptops and Ironkeys must always be carefully looked after to minimise the possibility of loss or theft, unauthorized use, or tampering.
- Ironkeys must be stored securely when not in use, but must never be stored or carried in the same bag as the laptop.
- Laptops must not be left in an unattended car or in an unsecured area.
- When a laptop is taken to a location such as hotel, the laptop must either remain with the person or be locked in the hotel room and, where possible, suitably secured with a cable lock.
- When taken home, the laptop must not be left in an obviously visible location but must be stored within the confines of a locked room/building. For added protection, a cable lock should also be used to physically secure the laptop.
- When using the laptop outside a formal secure area, consideration must be given to the possibility of eavesdropping or snooping. Staff must only use the laptop when it is safe to do so, particularly when entering passwords and should be mindful of the risk posed by surveillance cameras. In public areas the threat of theft or mugging should also be considered. (Consider the precautions you take when using an ATM, for example.)
- The laptop and Ironkey remain the property of IT Assist and must only be used for official purposes.
- Staff must ensure that their laptop is not used by anyone else.
- Ironkeys issued to individual members of staff for authentication of their laptops are associated with their email accounts and must not be given to or shared with any other person.

- Staff are reminded that their Ironkey must only be used for temporary offline storage of information in line with Departmental Records Management policy. It is not to be used as a backup storage device or for the long term storage of information. Storage of any personal or sensitive information, even on a temporary basis, must be approved by the Information Asset Owner (IAO).
- Laptops for training purposes are allocated to an individual member of staff who is responsible for ensuring that appropriate security controls are in place for the security and management of the Ironkey e.g. sign-in/sign-out procedures. Sensitive/personal data must not be held on laptops used for training purposes.
- Laptops for external presentations with associated Ironkeys are available from IT Assist. In this case, the Ironkey is allocated to an individual responsible for ensuring that appropriate security controls are in place for the security and management of the Ironkey e.g. sign-in/sign-out procedures. In this case the Ironkey does not have a PIN number associated with it. These laptops only have basic Microsoft Office installed and are intended for occasional use only. Only information necessary for the presentation should be held on the laptop and erased when no longer required.
- Additional Ironkeys required for data storage are available from IT Assist through the IT Assist Service Request Procedure.
- Additional Ironkeys may also be supplied on a temporary basis for a specific business use, for example, data transfer.
- Where a laptop is no longer required by its original recipient, the laptop and associated Ironkey must be returned to IT Assist for secure erasure, reloading of software, re-encryption and redeployment. The laptop and Ironkey must not be retained by the Branch as a spare.
- In exceptional circumstances there may be a requirement for a laptop and Ironkey 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 laptop and Ironkey. It is also their responsibility to ensure that this is recorded in an auditable, business process. The Departmental ITSO and IT Assist must be informed.
- IT Assist may monitor the use of laptop computers for purposes of security and administration.

4.3. OFFICE PROCEDURES

- A cable lock is supplied with the laptop. Users must ensure that their laptop is secured with this 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 by pressing ‘ctrl + alt+ del’ and choosing ‘lock this computer’.

- 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**.

5. ENCRYPTED DEVICES

- Only external media products officially approved for use can be connected to the laptop. The NICS has approved the use of Ironkey USB drives for secure portable data storage.
- A member of staff with a requirement to store, transfer or transport a volume of data larger than that offered by the NICS standard Ironkey must use a hard drive encrypted to the appropriate standard as detailed below.
- Departmental ITSOs and IAOs in business areas must ensure that external hard drives used to store data are appropriately encrypted as follows:
  - Personal or sensitive data must use CESG encryption (this policy document is not relevant to levels above Official - Sensitive); and
  - All other data must use encryption to FIPS-140-2 standard as a minimum.

6. BLACKBERRY SMARTPHONES

- Security accreditation for the BlackBerry smartphones allows for business email use. NICS policy permits users (authorised at Grade 5) to connect BlackBerry handsets to laptops or desktop PCs via USB to manage/transfer files**.** Local synchronisation is not permitted.
- Care must be taken when using the BlackBerry in public places. It must not be left unattended and the screen must be locked when not in use. Do not allow others in the vicinity to see the information displayed on the screen, particularly passwords and information which is personal or sensitive.
- Staff must only take their BlackBerry outside the UK when there is a business requirement to do so. Users must inform their Grade 5 (or above) before travelling.
- Whilst official encrypted BlackBerrys can be used to transmit emails containing personal or sensitive information, be aware that telephone calls are transmitted over open lines.
- Bluetooth can be enabled making hands free operation available when required. Bluetooth should be switched off when not in use. Users should be aware of the safety advice concerning hands free operation.
- Users with a business requirement for Wi-Fi should submit a service request authorised by their Grade 5 to IT Assist. Staff need to be aware that this presents a

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

security risk by opening the device to others using the same network. Wi-Fi should be disabled when not required.

- Blackberry Messenger is available for text only.
- Loss or theft of your BlackBerry must be reported immediately to IT Assist (0300 1234155 if external to the network, email itassist@nigov.net) so the 'lock and wipe' feature can be activated to disable the device, including the media card. All information held on a BlackBerry (including the media card) must be securely removed before disposal or reuse**.**
- Staff must not allow anyone else to use their BlackBerry and must not load any applications, other than those approved and managed by IT Assist, onto their device.

7. ALL OTHER DEVICES

As part of the NICS Lockdown process, use of the following devices is prohibited unless the specific application for use has been approved by the Grade 5 and the departmental ITSO, and agreed by IT Assist.

This list is not exhaustive, when in doubt seek advice from your departmental ITSO or IT Assist.

- Digital cameras, other than those 'read only' devices provided for business purposes
- Multi-media data storage cards (e.g. SD, MicroSD, Compact Flash).
- Mobile Phones/PDAs with local synchronization
- Tablets including iPads
- Connection of iPods/MP3 players
- Bluetooth or Wi-Fi connections with the exception of the BlackBerry (see Section 6)
- Unencrypted External Hard Drives
- USB drives (other than Ironkeys provided by IT Assist)
- BlackBerry Smartphones with local synchronization
- Webcams and USB headsets unless approved and installed by IT Assist. (Note: Enterprise Design Team (EDT) have a small list of approved devices DF1/12/16538)
- CDs/DVDs with write capability (Read is still permitted)

7.1 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 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.

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

- Multi-Media Data Cards (other than those used within BlackBerry Smartphones) must not be used to transfer or store NICS information. This includes the use of memory cards found in devices such as mobile phones, cameras and PDAs. Where there is a need to transfer or undertake short-term storage of information then an approved Ironkey issued by IT Assist must be used.

7.3. MOBILE PHONES

- Mobile phones must not be used to store or transfer NICS information. Local synchronisation with these devices is not permitted.
- These devices must not be connected to the NICS network, any NICS system or any NICS PC or laptop.
- Consider the sensitivity of personal contact details and messages stored on your mobile phone and where appropriate use a BlackBerry handset.
- Details of contact details for work colleagues and work related messages must be securely removed from your mobile phone before disposal or re-use.

7.4. TABLETS (E.G. APPLE IPAD)

- Tablet computers including the Apple iPad are not approved for connection to the NICS network (which in turn connects with PSN) as they do not meet CESG policy on data security or compliance with Data Protection Regulations.

7.5. APPLE IPODS/MP3 DEVICES

- iPods and other MP3 devices must not be connected to any NICS laptop or desktop PC.

7.6. BLUETOOTH

- Bluetooth connections must not be enabled on any IT Assist provided device other than the BlackBerry, where hands free operation is available if required.

7.7. WI-FI

- Wi-Fi connections must not be enabled on any IT Assist provided device other than by exception for the BlackBerry, where Grade 5 approval is required.

7.8 DIGITAL PENS

- Digital Pens are not approved for use with personal or sensitive data. If Digital Pens are to be used EDT/ESS should be contacted for advice on currently available encrypted devices. Grade 5 approval is also required.

8. SECURE REMOTE ACCESS (SRA)

- Any request for SRA must be approved by a Grade 5 prior to the Service Request being raised with IT Assist.
- Only NICS provisioned SRA facilities on a NICS provided laptop can be used to gain access to NICS systems from outside the regular office environment.
- For Secure Remote Access, users MUST only use Internet Explorer to ensure compliance with the internet access security policy.
- If you suspect that the PIN on your Cryptocard has been compromised or the Cryptocard has been lost you must report this to the Departmental ITSO. The IT Assist Helpdesk (155) must also be contacted to request a PIN change or report the loss.

9. TRAVELLING ABROAD

Encrypted devices including laptops and Ironkeys **MUST ONLY** be taken outside the UK when there is a business requirement and approval from the Grade 5.

- Staff are required to read HMG IA Standard No 4, Supplement 8 before seeking approval. This standard is available from your Departmental ITSO.
- If travelling or working overseas, contact your ADSO or ITSO to check whether additional security restrictions apply.
- The Departmental ITSO and IT Assist must be informed.

10. ASSET MANAGEMENT

- All devices must be recorded on the Assets Register and managed in accordance with the procedures in 'Guidance on Security of Portable Assets', which can be found at http://itassist.nigov.net/index/management_information/index/management_information/itassist-guidance-on-security-of-portable-assets.doc
- Any breach of this policy will be viewed as a security incident and dealt with as such, possibly leading to disciplinary action.

11. PASSWORD MANAGEMENT

- Users must memorise their BitLocker PIN and password before taking the laptop out of the secure office environment[3]. Likewise users of BlackBerrys and other approved devices must memorise passwords/PINs.
- Users must not share passwords/PINs with others.
- If you suspect that your password/PIN has been compromised you must report this to the Departmental ITSO and contact the IT Assist Helpdesk (155 from inside network or 0300 1234155 from outside the network) to request an immediate password/PIN change.
- If you forget your password, contact IT Assist Helpdesk to request a reset.

12. 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 IS THE DOJ WHO OPERATE WITHIN THE IT ASSIST CONFIDENTIAL (ITAC) NETWORK. AS A RESULT OF IL4 AND CONFIDENTIALITY REQUIREMENTS HIGHER LEVELS OF SECURITY AND ENCRYPTION ARE REQUIRED OR IN SOME CASE ASPECTS OF MOBILE FUNCTIONALITY PROHIBITED. THIS IS CURRENTLY UNDER REVIEW.**

13. INCIDENT REPORTING

- **ALL INCIDENTS OR BREACHES OF SECURITY MUST BE REPORTED IMMEDIATELY** or as soon as reasonably possible to IT Assist (03001234155 if external to the network, email itassist@nigov.net)
- 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 Badge Number and contact information needed in an emergency to report if the laptop is lost or stolen.
- Users should attempt to power down and secure the laptop 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, Ironkey or other mobile device must be reported at the earliest opportunity to the Departmental ITSO, who will advise on the action that must be taken, and also to IT Assist. The

[3] Your Departmental ITSO can be consulted for further guidance or if staff have difficulty complying.

ITSO must immediately undertake a "Damage Assessment", which will include a review of the security of the laptop, mobile device, associated passwords and the Ironkey, to determine whether security may have been comprised. As part of the damage assessment the protective marking of the information stored will be recorded.

- Departmental ITSOs must report the loss of encrypted laptops, Ironkeys or any mobile device using encryption to the NICS Crypto Custodian and ensure that the appropriate incident form is completed as soon as possible. The loss or theft of a laptop must also be reported to the police. The PSNI incident number should be included on the incident form.
- Users are not authorised to change the system configuration or the hardware profile.
- 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[4].
- 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 details on who is permitted to manage security functionality refer to the IT Assist Helpdesk (155)

14. TRAINING

- When issued with a laptop, users will be given appropriate instructions on the use of the security functionality and their responsibility for safeguarding the laptop and Ironkey.
- If further guidance is required please contact your Departmental ITSO.

15. ELECTRONIC DOCUMENT AND RECORD MANAGEMENT

- In line with NICS Policy, information should be stored on RecordsNI (TRIM), 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 IL3 level must not be input or stored. The Departmental Information Manager (DIM) should be contacted for further guidance.

[4] 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.

16. STAFF MOVES, REUSE 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** laptops and 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).
- You should contact your departmental ITSO if you require any further advice.

17. 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 IT Assist in the first instance. Issues concerning the policy will be referred through IT Assist Tel. 155 (or 0300 1234155 if external to the network) email itassist@nigov.net to the Central Information Assurance Team email isid.iateam@dfpni.gov.uk.