PS 176 Removable Media Policy

December 2013

Version 2.0

Statement of legislative compliance

This document has been drafted to comply with the general and specific duties in the Equality Act 2010; Data Protection Act; Freedom of Information Act; European Convention of Human Rights; Employment Act 2002; Employment Relations Act 1999, and other legislation relevant to policing.

Table of Contents

Aims and Objectives of the Policy

Aims and Objectives

Nottinghamshire Police will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting Force business.

This policy applies to all Nottinghamshire Police Officers, Police Staff, Partners, agents and approved persons working for or with the Police who have access to Nottinghamshire Police information, information systems or IT equipment and intends to store any information on removable media devices.

This policy should be adhered to at all times, but specifically whenever any user intends to store any information used by the Force to conduct official business on removable media devices

The main aims and objectives are to:

- Enable the correct data to be made available where it is required.
- Maintain the integrity of the data.
- Prevent unintended or deliberate consequences to the stability of Nottinghamshire Police computer network.
- Avoid contravention of any legislation, policies or good practice requirements.
- Build confidence and trust in the data that is being shared between systems.

- Maintain high standards of care in ensuring the security of personal, protected and Restricted information.
- Enable the disclosure of information as may be necessary by law.

Policy statement

List of Removable Media devices

Removable media devices include, but are not restricted to the following:

- CDs.
- DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

Risks

Nottinghamshire Police recognises that there are risks associated with users accessing and handling information in order to conduct official Force business. Information is used throughout the Force and sometimes shared with external organisations and applicants. Securing RESTRICTED and personal data is of paramount importance – particularly in relation to the Force's need to protect data in line with the requirements of the Data Protection Act 1998. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of the Force. It is therefore essential for the continued operation of the Force that the confidentiality, integrity and availability of all information recording systems are maintained at a level, which is appropriate to the Force's needs

This policy aims to mitigate the following risks:

- Disclosure of RESTRICTED or personal information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of Force networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the Force or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the Force or individuals as a result of information loss or misuse.
- Damage to Nottinghamshire Police's reputation and loss of public trust and confidence as a result of information loss or misuse.

Non-compliance with this policy could have a significant effect on the efficient operation of the Force and may result in financial loss and an inability to provide necessary services to our customers.

Restricted Access to Removable Media

Senior Managers are responsible for ensuring that local procedures are in place for the management of all removable media devices. There are large risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given.

Requests for access to, and use of, removable media devices must be made using Forms G791 / 792 / 793 as appropriate. Approval for their use must be given by line managers.

Should access to, and use of, removable media devices be approved the following sections apply and must be adhered to at all times.

Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by the Information Services via the call-off contract. Non-force owned removable media devices must not be used to store any information used to conduct official Force business, and must not be used with any Force owned or leased IT equipment.

Any equipment purchased outside of the Call-off Contract arrangements must not be attached to the Force IT network. Attaching un-authorised equipment to our network could present a risk of conflict and the failure of other Force systems. All equipment ordered through the Call-off Contract arrangements is tested to ensure they are compatible with our existing systems and capable of being supported by our technical staff and existing resources.

Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable or corrupted through loss, destruction or malfunction of equipment than data that is frequently backed up. Therefore removable media should not be the only place where data obtained for Force purposes is held. Copies of any data stored on removable media must also remain on the source system or networked computer until the data is successfully transferred to another networked computer or system.

In order to minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment in line with the protective marking of the data.

Each user is responsible for the appropriate use and security of data and for not allowing removable media devices, and the information stored on these devices, to be compromised in any way whist in their care or under their control.

All data stored on removable media devices must, where possible, be encrypted.

Users should be aware that the Force may audit / log the transfer of data files to and from all removable media devices and Force-owned IT equipment.

The following controls should be applied to a standard consistent with that required by the protective marking of the media stored on the removable media device:

- When no longer required, the contents of any removable media device that are either to be used elsewhere, or removed from within the force, should be erased.
- Media containing protectively marked or other sensitive information should only be removed from force premises only with authorisation by line management. A record of all such removals should be kept in order to facilitate an audit trail.
- All media should be stored in a safe, secure environment, in accordance with the protective marking of the media's contents, and with any manufacturer's specifications relating to the media

Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security, this includes any misuse or irresponsible actions that affect business data and any actual loss of data to the Force Information Security Manager as soon as practicable.

Third Party Access to Force Information

No third party (external contractors, partners, agents, the public or non-employee parties) may receive data or extract information from the Force's network, information stores or IT equipment without an appropriate Information Sharing Agreement being in place.

Should third parties be allowed access to Force information then all the considerations of this policy apply to their storing and transferring of Force data.

Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the Service Desk (Information Services) in the first instance should removable media be damaged.

Virus and malware checking software approved by the Information Services must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded.

Whilst in transit or storage the data held on any removable media devices must be given appropriate security according to the type of data and its sensitivity. Encryption or password control must be applied to the data files unless there is no risk to the Force, other organisations or individuals from the data being lost whilst in transit or storage.

Disposing of Removable Media Devices

Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage. Any previous contents of any reusable media that are to be reused within the Force must be erased. This must be a thorough removal of all data from the media to avoid potential data leakage using specialist software and tools. All removable media devices that are no longer required, or have become damaged, must be returned to the Information Services for secure disposal.

For advice or assistance on how to thoroughly remove all data, including deleted files, from removable media contact the Service Desk (Information Services).

User Responsibility

All considerations of this policy must be adhered to at all times when using all types of removable media devices. However, special attention must be paid to the following when using USB memory sticks (also known as pen drives or flash drives), recordable CDs, DVDs and diskettes:

- Any removable media device used in connection with Force equipment or the network or to hold information used to conduct official Force business must only be purchased and installed by Information Services via the call-off contract. Any removable media device that has not been supplied by Information Services must not be used.
- All data stored on removable media devices must be encrypted where possible.
- Virus and malware checking software must be used when the removable media device is connected to a machine.
- Only data that is authorised and necessary to be transferred should be saved on to the removable media device. Data that has been deleted can still be retrieved.
- Any Removable media devices used for archiving or storing records as an alternative to other storage equipment must be identified tot eh Information Services Department
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Compliance

If any user is found to have breached this policy, they may be subject to disciplinary action. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Security Team

Key Messages

- The use of removable media devices is only be approved if there is a valid business case for its use.
- Any removable media device that has not been supplied by Information Services must not be used.
- All data stored on removable media devices must be encrypted where possible.
- Damaged or faulty removable media devices must not be used.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage.
- Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to avoid data leakage

Related documents and Appendices

PS 177 Remote Working Policy

Administration

Version Control

Section changed	Details of change

Monitoring and review

Measure	Date/period and process of review

Registered Owner

Owner	Author
Deputy Chief Constable as Senior Information Risk Officer (SIRO)	Information Security Manager