

 WARWICKSHIRE POLICE		POLICY
Security Classification	OFFICIAL	
Disclosable under Freedom of Information Act 2000	Yes	

POLICY TITLE	Removable Media
REFERENCE NUMBER	WP307
Version	2.1

POLICY OWNERSHIP	
DIRECTORATE	Data, Strategy and Technology
BUSINESS AREA	Digital Services

INITIAL IMPLEMENTATION DATE	April 2015
NEXT REVIEW DATE:	August 2027
RISK RATING	MEDIUM
EQUALITY ANALYSIS	LOW
TIER	2

Warwickshire welcome comments and suggestions from the public and staff about the contents and implementation of this policy.
Please e-mail policiesandprocedures@warwickshire.police.uk

1.0 POLICY OUTLINE

Warwickshire 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 official police business.

2.0 PURPOSE OF POLICY

The policy establishes the principles and working practices that are to be adopted by all users for data to be safely stored and transferred on removable media.

This policy aims to ensure that the use of removable media devices is controlled 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 the forces' 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 sensitive information.
- Avoid the disclosure of information as may be necessary by law.

3.0 IMPLICATIONS of the POLICY

This policy applies to all officers, staff, contractors, and volunteers of each force who have access to police information, information systems or IT equipment and intend to store any information on removable media devices.

3.1 Definition

This policy should be always adhered to, but specifically whenever any user intends to store any information used by Warwickshire Police to conduct official business on removable media devices.

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

- CDs
- DVDs / Blu-ray
- SD-cards and variants
- Optical Disks
- External Hard Drives (including Solid State 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)
- Smartphones
- MP3 Players
- Digital Cameras
- Backup Tapes
- Audio Tapes (including Dictaphones and Answering Machines)
- Legacy Floppy disk drives

3.2 Risks

Warwickshire Police recognise that there are risks associated with users accessing and handling information to conduct official force business. Information is used throughout the force and sometimes shared with external organisations and applicants.

Securing sensitive data is of paramount importance – particularly in relation to the Police need to protect data in line with the requirements of the Data Protection Act 2018 (see Data Protection Policy), and UK GDPR. Any loss of the ability to access information or interference with its integrity could have a significant effect on the efficient operation of Police business. It is therefore essential for the continued operation of the Police business, that the confidentiality, integrity, and availability of all information recording systems are maintained at a level, which is appropriate to Police needs and in line with protective marking requirements.

This policy aims to mitigate the following risks:

- Disclosure of sensitive information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of police networks or equipment through the introduction of malware including viruses, through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the police or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the police or individuals as a result of information loss or misuse.
- Reputational damage as a result of information loss or misuse.
- To achieve compliance to industry standards

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.

4.0 PROCEDURE

4.1 Restricted Access to Removable Media

It is policy to restrict the use of all removable media devices. The use of removable media devices must only be for valid business reasons. There are significant risks associated with the use of removable media, and therefore clear business benefits that outweigh the risks must be demonstrated before approval is given. Digital services should be consulted prior to new removable media use. They will in turn liaise with Information Assurance and provide appropriate guidance.

Should access to, and use of, removable media devices be required the following sections apply and must be always adhered to.

4.2 Procurement of Removable Media

All removable media devices and any associated equipment and software must only be purchased and installed by Digital Services, except where alternative arrangements are made in writing with the Cybersecurity Architect. In principle, non-force owned removable media devices should not be used. Where there is an operational need to use such, advice should be sought first from Digital Services.

4.3 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 which is frequently backed up. Therefore removable media should not be the only place where data obtained for police 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.

To minimise physical risk, loss, theft or electrical corruption, all storage media must be stored in an appropriately secure and safe environment. Consideration should also be given to storage conditions, which should not be subject to extremes of temperature or moisture – manufacturers recommendations should be followed in this regard. Data identified for long term retention should be stored at Defford and comply with storage guidance.

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 whilst in their care or under their control.

All data stored on removable media devices should be encrypted.

It is acknowledged that in some circumstances, encryption is not appropriate, for example, where it may contravene the ACPO principles of digital evidence. Where encryption is not possible, guidance should be sought from the Cyber Security Team prior to data being transferred to removable media. All alternative options should be considered prior to using removable media for unencrypted data, as this could potentially pose significant risk to the force.

4.4 Incident Management

It is the duty of all users to immediately report any actual or suspected breaches in information security to the Information Assurance Team via the Security Incident Reporting Form (SIR1) and to Digital Services.

Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident.

4.5 Third Party Access to Police Information

Authorised third parties (external contractors, partners, agents, and the public or non-employee parties) may receive data or extract information from the police network, information stores or IT equipment where there is a legal/contractual or other lawful basis to share in place. You should contact the Information Assurance Team to discuss if a DPIA/Sharing Agreement or contract is needed.

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

4.6 Preventing Information Security Incidents

Damaged or faulty removable media devices must not be used. It is the duty of all users to contact the Digital Services Service Desk should removable media be damaged.

Modern malware protection 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. The data must be scanned by virus checking software products before the media is loaded on to the receiving machine. 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 and password control must be applied to the data files.

4.7 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 by Digital Services. 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 Digital Services Service Desk for secure disposal following the secure disposal policy.

4.8 User Responsibility

All considerations of this policy must be always adhered to 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), external hard drives, smartphones, recordable CDs, DVDs and legacy diskettes:

- Any removable media device used in connection with Police equipment or the network or to hold information used to conduct official Police business **must** only be purchased and installed by Digital Services.
- All police data stored on removable media devices **must** be encrypted, especially, when it is sent to external agencies / partner organisations
- 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.
- Removable media devices **must not** be used for archiving or storing records as an alternative to other storage equipment.
- 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.
- For advice or assistance on how to securely use removable media devices, please contact the Digital Services Service Desk.

5.0 CONSULTATION

Consultation has taken place with:

Director of Data, Strategy and Technology
 Head of Digital Services
 Head of Information Assurance
 Head of Service Management
 Cyber Security Architect
 Infrastructure Architect
 Network Architect

6.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart:

Date	Author / Reviewer	Amendment(s) & Rationale	Date of Approval / Adoption
23.3.15	Paul Williams	Harmonisation	JNCC 02/04/2015
25.5.17	Ranjit Singh	Reviewed Amendment to 4.8 – All police data stored on removable media devices must be encrypted, especially, when it is sent to external agencies / partner organisations	23/06/2017
30.11.23	James Morgan-Jones	Updated to single force, updated departments, and terms. Reviewed and added clarification where required.	
13.02.24	James Morgan-Jones	Updated following review with force ISO and Cyber Security Consultant	
12.12.24	James Morgan-Jones	Minor changes for adoption	
10/06/2025	James Morgan-Jones	Final update for Board approval. Replaces A080	12/08/25. Governance Board approved.

7.0 ASSESSMENT AND ANALYSIS

The Equality Analysis (EA), Health & Safety Assessment (HAS) and Risk Assessment (RA) associated with this document are available on request.