



PORTABLE DATA STORAGE DEVICES STANDARD OPERATING PROCEDURE (SOP)

| STANDARD OPERATING PROCEDURE | | | |
|------------------------------|---|---|---------------|
| REFERENCE. | SOP/193/09 | | |
| PROTECTIVE MARKING | Not Protectively Marked | | |
| PORTFOLIO | Deputy Chief Constable | | |
| OWNER | Head of Professional Standards Department | | |
| START DATE | 2 November 2009 | | |
| REVIEW DATE | September 2012 | | |
| THIS POLICY REPLACES: | SOP/117/08 | | |
| VERSION | DATE | REASON FOR AMENDMENT | AMENDED BY |
| 1.3 | 11 Sept 2009 | Due for Review. This was done earlier than scheduled to address different concerns raised with the content of the previous SOP. | Gary Williams |



CONTENTS

| | | |
|-----|--|----|
| 1 | INTRODUCTION | 3 |
| 2 | KNOWLEDGE | 4 |
| 2.1 | Terms and Definitions..... | 4 |
| 2.2 | Responsibilities | 5 |
| 3 | PROCEDURES | 5 |
| 3.1 | Operating Procedures | 5 |
| 3.2 | Use of PDSs | 7 |
| 3.3 | Software Security | 9 |
| 3.4 | Hardware Security | 10 |
| 3.5 | Physical Security | 10 |
| 3.6 | Fault Reporting | 11 |
| 3.7 | Incident Management/Reporting Procedures | 11 |
| 3.8 | Security Contact | 11 |
| 4 | MONITORING AND COMPLIANCE | 12 |
| 5 | APPENDICES/ASSOCIATED DOCUMENTS | 12 |



PORTABLE DATA STORAGE DEVICES STANDARD OPERATING PROCEDURE

1 INTRODUCTION

- 1.1 These procedures provide guidance in relation to the use of Portable Data Storage Devices (PDSDs) and enforce the conditions of the Information Security Policy.
- 1.2 The use of PDSDs has increased significantly in both domestic and business environments. The drivers for this increase include ease of use, improved functionality, and greater storage capacity and low cost. However, like many new technologies, the introduction of PDSDs brings with it increased security risks. Failure to address these risks can result in a range of incidents, including loss of British Transport Police (BTP) information, unlawful disclosure, tampering of key records and the introduction of viruses and other malicious software
- 1.3 The purpose of this Standard Operating Procedure (SOP) is to:
- Identify controls to help protect the use of PDSDs;
 - Ensure that BTP information is properly protected, to protect our staff against the consequences of losing devices containing BTP information;
 - To clarify the ownership of devices and information.
- 1.3 This procedure applies to England, Wales and Scotland.
- 1.4 This procedure applies to all BTP employees, volunteers, members of other agencies and those acting as our servants or agents who have authorised access to BTP information.



2 KNOWLEDGE

2.1 Terms and Definitions

2.1.1 **PDSs** are portable devices which are relatively easy to use and can hold high volumes of data.

PDSs can be grouped into three types:

- 1) Integrated storage devices, ie where the storage media and read/write components are housed within a single integrated unit, (e.g. USB memory sticks, digital pens, external hard disks);
- 2) Personal electronic devices (PEDs) with data storage capabilities (e.g. digital cameras, portable media players, digital voice recorders);
- 3) Storage devices with separate removable media (e.g. Zip disks, CD/DVD writers, Flashcards).

2.1.2 **Information Asset** is any data or information that has value to BTP. This can take many forms whether written on paper or stored electronically.

2.1.3 **Confidentiality** - Assurance that information is shared only among authorised persons or organisations. Breaches of confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned.

2.1.4 **Integrity** - Assurance that the information is authentic and complete. The integrity of data is not only whether the data is correct but whether it can be trusted and relied upon.

2.1.5 **Availability** - Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.



2.1.6 **Personal Data** - Information relating to or that can identify an individual

2.2 Responsibilities

2.2.1 The Deputy Chief Constable is responsible for ensuring the Confidentiality, Integrity and Availability of information assets and promoting these procedures throughout BTP.

2.2.2 The FISO is responsible for establishing information security policies, procedures and standards for BTP and implementing processes in line with the Association of Chief Police Officers (ACPO) Community Security Policy for the Police Community.

2.2.3 Where PDSDs are issued Departmental Heads and Area Commanders should ensure that staff follow established procedures and should report any non compliance with policies and procedures to the Force Information Security Officer (FISO).

3 PROCEDURES

3.1 Operating Procedures

3.1.1 These procedures apply to all staff that use any form of PDSDs and apply to devices that are owned and issued by BTP.

3.1.2 These procedures do not include the use of Mobile Data Terminals or Blackberry phones for which separate guidance and security procedures are available or personally owned PDSDs as no personally owned PDSDs can be used to process BTP information.

3.1.3 These procedures do not preclude the use of CDs/DVDs, merely the USB devices e.g. ZIP Drives etc being connected to the Network. However staff should follow the



guidance in CESG Good Practice Guide No 3 – Securing Bulk Data, in processing protectively marked and personal data

3.1.4 PDSDs especially USB memory sticks will be permitted only by exception, consequently these will not be issued as a matter of course. One or more of the following requirements must be met:

- There is no other way of transferring the data: alternative methods may include a secure FTP (File Transfer Protocol) Link, Secure Remote Access, and burning data onto CD/DVDs, (further guidance in relation to Securing Bulk Data Transfer – CESG Good Practice Guide No 3 and Protecting Personal Data and Managing Information Risk -Infosec Standard No 6 is available from the Force Information Security Officer)
- The information transferred to any removable media should be the minimum necessary to achieve the business needs, both in terms of the numbers of people covered by the information and the scope of information held. Where possible, only anonymised information should be held;

3.1.5 Users of PDSDs are responsible for security of the hardware and information held on it. Users must report any breach of security involving the device, its components or information held on the device itself in accordance with the procedures in the Force Information Security Policy and Manual. All losses of PDSDs should be reported to the Technology Department and to Informationsecurity@btp.pnn.police.uk using the Security Incident Reporting Procedures

3.1.6 Users are responsible for ensuring that all personal data held on PDSDs complies with the Data Protection Act, 1998. In addition users are reminded of their



obligations, if applicable, on “disclosure” under the Criminal Procedure and Investigations Act, 1996; and the Code of Practice.

3.2 Use of PDSs

3.2.1 The use of any PDS Device which has not been issued or registered by the Technology Department is totally forbidden.

3.2.2 Staff wanting to use PDSs not procured via technology (portable electronic devices with storage e.g. cameras) will still have to register them as the monitoring software will not allow them to be used on the Force Network unless they are registered.

3.2.3 Users must only use BTP issued PDSs for official purposes.

3.2.4 Users must not load personally owned data or other unauthorised software onto PDSs (including Internet software).

3.2.5 The forces’ Regional Information Security Officers will use the list of issued and declared PDS to audit compliance. Any undeclared PDSs or personal PDSs found to have BTP information will result in disciplinary action being taken against the individual.

3.2.6 It should be noted that the purchase of digital cameras remains an Area responsibility, but must be done in consultation with the BTP Photographic Department (part of Scientific Support). This will ensure that the necessary quality and specification/equipment are adhered to, as per the BTP Digital Cameras Procedure.



3.2.7 With regards to PDSs the Technology Department will only issue two types of USB memory sticks. These are:

- USB for Non Protectively Marked (PM) Information - Password protection
- USB for PM Information up to RESTRICTED/Personal Data - encryption

3.2.8 Good business continuity practice dictates that, regardless of the type of USB device used, it will only be used to store information temporarily. All data copied to a USB device must also be backed up to the user's H drive or deleted as soon as reasonably practicable. The changes which have been made to the files, whilst working away from the office, should be backed up on users H drive when users are next in the office.

3.2.9 BTP issued USB memory sticks should only be used in conjunction with BTP equipment. The use of BTP issued memory sticks with non-BTP equipment is forbidden

3.2.10 Users are reminded that usage of all PDSs will be monitored by specialist auditing software when connected to the Force Network. This will provide the force with an audit trail of exactly what the user has imported or exported from the device.

3.2.11 PDSs will not be authorised, activated or recognised by the Force Network until the completed form (Appendix A) is received by the Technology Department.



3.2.12 PDSDs issued must only be used for as long as the business purpose exists. When no longer required they must always be returned to Technology and not given to any other person as they are only authorised on the system for a particular user. Where Technology intend to re-issue a PDSD they will ensure that there is no residual data on the device.

3.2.13 Desktops are configured to scan memory sticks on access for viruses.

3.2.14 Dictaphones are not to be used as a mass data storage device.

3.3 Software Security

3.3.1 Where a PIN code/Password is required this must be utilised at all times. In the case of USB memory sticks, users will be issued with a randomly generated password. Users **will not** change the password once the device has been issued by the Technology Department. If this password is forgotten, users should contact the Technology Service Desk. It should be noted that users will be asked for details of their date of birth for verification purposes and passwords will be re issued only via the force email system. BTP is committed to ensuring that only legal and properly purchased and authorised software is used on its systems.

3.3.2 The software installed on PDSDs will comply with all legal and statutory requirements applicable to the use of copyrighted computer software products in accordance with the Technology Department's Software Compliance Policy.

- Users **must not** install, attempt to install or use any additional software on PDSDs, even if that software has been properly purchased and licensed for BTP use. Any additional installations must be carried out by the technology department.



- Users **must not** use or attempt to access and use any other programs that may be installed on the device.
- Users **must not** attempt to access the BTP Network or any other stand alone system with a PDS without authorisation.

3.4 Hardware Security

3.4.1 The back of any issued USB device should be marked with the following:

“Please return to Freepost Tech”

3.4.2 Users must record the asset and serial number of the device. This is so such information can be given to police or support staff immediately if the device is stolen or lost, rather than waiting to get the information from the corporate inventory or other source.

3.4.3 PDSs due to their compact size, are easy prey for physical theft from the person or buildings (offices, rooms, etc). They are also easy to lose through simple carelessness. The following are “handy hints” to try and minimise the risk:

- **Do not** place them in pockets or open bags, etc;
- **Do not** leave them on display in vulnerable places such as vehicles, rooms, or offices;
- When not in use **keep them out of sight** - preferably locked away.
- USB Memory Sticks should not be attached to keys.

3.5 Physical Security

3.5.1 Users are responsible for the physical security of devices and when not in use the device **will be** stored secured commensurate with the highest protective marking of data held on the device.



3.6 Fault Reporting

3.6.1 Any faults with the equipment must be reported to the Technology Service Desk. If a device requires the attention of an engineer it **will** be brought into the place of work or other agreed BTP premises. Engineers **will not** undertake visits to non-BTP locations. It is user's responsibilities to ensure that PDSDs are available for maintenance purposes.

3.7 Incident Management/Reporting Procedures

3.7.1 All incidents relating to the security of PDSDs must be brought to the attention of line management, who in turn should notify the Information Security Unit.

3.8 Security Contact

3.8.1 The following contact numbers should be used regarding any security issue

| | |
|---|-------------------------|
| Technology Service Desk | 004 8899 – 0207 8308899 |
| Force Information Security Officer | 058 4935 |
| Regional Information Security Officer (LU/LN) | 004 6916 |
| Regional Information Security Officer (LS/WW) | 089 8210 |
| Regional Information Security Officer (NE/NW/S) | 038 3482 |



4 MONITORING AND COMPLIANCE

- 4.1 This SOP will be monitored by the FISO to ensure compliance with BTP policy and procedures in relation to Information Security.

5 APPENDICES/ASSOCIATED DOCUMENTS

- 5.1 [Force Information Security Policy](#)
- 5.2. Force Information Security Manual
- 5.3 [Appendix A – Request/Approval for USB Storage Device](#)



**APPENDIX A REQUEST/APPROVAL FOR
PORTABLE DATA STORAGE DEVICE**

| | | | |
|--|--------------------------|--|--------------------------------|
| Part 1 - Requestor Details | | | |
| Name: | | Rank/Police No: | |
| Area: | | Contact No: | |
| Signed: | | IT Ref No: | |
| Business Requirement | | | |
| Portable Data Storage Device Type | | What is the proposed use of the storage device? | |
| USB STICK | <input type="checkbox"/> | | |
| USB HARD DRIVE | <input type="checkbox"/> | | |
| DICTAPHONE | <input type="checkbox"/> | | |
| OTHER (Please Specify) | <input type="checkbox"/> | | |
| What is the highest protective marking of the data that will be transferred to the USB storage device? Not Protectively Marked <input type="checkbox"/> Restricted and Above <input type="checkbox"/> | | | |
| In accordance with the SOP the preferred solution to transfer data would be secure FTP (File Transfer Protocol) Link, Secure Remote Access, or burning data onto CD/DVDs. Please specify why you cannot use this form of media | | | |
| Does the requestor have access to a Force laptop? | | Yes <input type="checkbox"/> | No <input type="checkbox"/> |
| Authorising Line Manager Details | | | |
| Police No | Signed | Block Capitals | Date |
| | | | |

| Part 2 – Issue Details/Return Details (delete as applicable) | | | |
|--|--------------------------|------------------------|--------------------------|
| Type of Portable Data Storage Device | | | |
| USB STICK | <input type="checkbox"/> | DICTAPHONE | <input type="checkbox"/> |
| USB HARD DRIVE | <input type="checkbox"/> | OTHER (please specify) | <input type="checkbox"/> |
| Make | | | |
| Model | | | |
| Serial No | | | |
| Additional Information | | | |

| Technology Staff Issuing/Receiving Details (delete as applicable) | | | |
|---|--------|----------------|------|
| Police No. | Signed | Block Capitals | Date |
| | | | |
| Issued/Returned to/by: (delete as applicable) | | | |
| Police No | Signed | Block Capitals | Date |
| | | | |

1. By signing this agreement the noted staff member agrees not to change any of the parameters on the PDS.
2. By signing this form the user acknowledges that they have read and understood the SOP for PDSs and are aware that any breach of this SOP will be treated as a disciplinary issue.
3. If the device is lost, the Force Control Room/Technology Service Desk must be notified immediately.
4. Any person found using an unauthorised PDS device and connecting such a device on the BTP Desktop/Laptop will be referred to the Professional Standards Department.
5. PDSs will not be activated for use on the Force Network until the signed form is returned.