

Warwickshire Police Authority – 26 May 2010

Management of Information Policy

Report of Lead for Publications and Information

Purpose and Supporting Documents

To ensure that the security clearance of the Authority's Members and Staff is compatible with that of the Force

Recommendation

That approval be given to the proposed Management of Information Policy

1. Introduction

- 1.1 The aim of this policy is to define the position of Warwickshire Police Authority in relation to **Information Management** and to identify practices which are both sensible and compatible with relevant legislation and Codes of Practice for the Management of Police Information (MoPI).
- 1.2 This policy applies to all Authority members and staff (including agency staff) and as such, they will be expected to comply with its principles.

2. Strategic Aim

- 2.1 To competently record and manage all information held by the Authority in an efficient and consistent manner in order to support the business activities of the Authority and the achievement of its objectives.

3. MoPI

- 3.1 The Warwickshire Police Force has comprehensive guidance on the Management of Information. The great majority of information held by the Force relates to individual people (eg offenders, suspects, witnesses and victims).
- 3.2 If the Forces does choose to share information about individuals with the Authority, such information should normally be deleted or destroyed by the Authority as soon as possible.
- 3.3 Adherence to the **Protectively Marked Material Policy** (see Appendix 1) will normally suffice as the Authority's compliance with the MoPI regulations.

4. Scope

- 4.1 The Authority will keep data records that are complete, authentic, reliable, secure and accessible and manage those records in accordance with good practice.
- 4.2 A record is defined as 'information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (BS ISO 15489 : 2001).
- 4.3 This policy applies to **all records** in any format created, received or maintained (including hard copy as well as electronic and digital formats or magnetic, digital, photographic and optical media).
- 4.4 Emails created, received or maintained by staff or members of the Authority in the course of carrying out the functions of the Authority, are covered by this policy.

5. Legal Compliance

- 5.1 The legal base for this policy is:

(a) **The Freedom of Information Act 2000**

This Act gives the public a general right of access to information held by public authorities. It also required such authorities to have an approved publication scheme, which is a means of providing access to information which an authority proactively publishes.

When responding to requests, there are procedural requirements set out in the Act which an Authority must follow. There are also valid reasons for withholding information, which are known as exemptions from the right to know.

(b) **Human Rights Act 1998**

Gives legal effect in the UK to the fundamental rights and freedoms contained in the European Convention of Human Rights (Sections 2 and 8).

(c) **Equality Act 2010**

Under this policy no person will be treated less favourable on the various grounds outlined in the Act.

(d) **Data Protection Act 1998**

The Act requires that **personal** information records must comply with the principles set out below:

- being fairly and lawfully processed
- being processed for limited purposes and not in any matter incompatible with those purposes
- be adequate, relevant and not excessive
- accurate, and where necessary, up to date
- not being kept longer than necessary
- being processed in accordance with individual rights
- not be transferred outside the UK.

6. Functions and Responsibilities

6.1 Chief Executive

The Chief Executive has overall responsibility for records management policy and standards.

6.2 Assistant Chief Executive

The Assistant Chief Executive has responsibility for the following:

- computer equipment, its maintenance and security, the IT system used and access to the internet. This responsibility is undertaken in conjunction with Warwickshire County Council;
- the Registered contact at the Authority in respect of the Data Protection Act and the Freedom of Information Act;
- to ensure that records will be readily available to meet the Authority's needs and legal obligations;
- to establish Data Quality Principles and the practice to be adopted in relation to retention and disposal;
- to issue to staff Codes of Practice in respect of email, internet and intranet.

6.3 All Members and Staff

- (a) Have responsibility to implement the Authority's Information Management Policy and standard working practices.
- (b) Ensure information is recorded, maintained and disposed of in accordance with local requirements.
- (c) Ensure correct GPMS marking.

7. Email

- 7.1 Unless passed over a secure network, the content of emails and attached documents should be regarded as being open to the public.

Hence information which is not suitable for the public domain should not be processed or stored on personal computing equipment.

Material marked as **restricted** or **confidential** should not be sent electronically to personal, unsecure email addresses.

8. Authority Website

- 8.1 The Assistant Chief Executive, with the support of the Authority Lead for Publications and Use of Information, will have responsibility for managing the content and updating the Authority's website.

All Members and Staff will be required to contribute appropriate content from time to time.

9. Government Protective Marking Scheme (GPMS)

- 9.1 Police authorities come under the Local Government Acts and, in most cases, proceedings (and papers) are open to the public in line with transparent and open government. There is provision whereby certain proceedings can be declared 'exempt' and thus are not openly reported. The general rule is that police authority business is open to the public.
- 9.2 The Warwickshire Police Force uses the Government Protective Marking Scheme and every document emanating from them is marked **Not Protectively Marked/Protect/Restricted/Confidential/Secret/Top Secret**.
- 9.3 This policy advocates that the Authority should adopt the same marking scheme in respect of information passed to the Force. Such a practice would establish a mutual understanding as to the sensitivity of information being passed or received.
- 9.4 In deciding the correct marking for any information, the initiator should consider how damaging the consequences would be if the material was lost, stolen, disclosed or destroyed. Further guidance is set out in **Appendices 1 and 2**.

Appendix 1

PROTECTIVE MARKING

All information for internal and partner use will be protectively marked using markings defined below. Members and employees must assess all information for a protective marking, based on risk and impact of disclosure. The protective markings to be used are:

1. **Not protectively Marked**

Anyone can access the information internally or externally. It may be published on the web or in paper form. The marking will be **Not Protectively Marked** or no marking at all.

2. **Protect**

Information where disclosure or unauthorised access would be inappropriate, inconvenient or cause harm or financial impact.

There will be clear marking on the information as **Protect**.

3. **Restricted**

Information to be restricted at a higher level of assurance than Protect, due to significant inconvenience, damage, harm or financial impact on the Authority or Force, or individuals.

There will be clear markings on the information as **Restricted**.

4. **Confidential**

More sensitive information than Restricted which could result in the loss of a criminal case, financial damage or injury or death to an individual.

Advice from an expert source may need to be sought in respect of handling, storage or disposal.

There will be clear markings on the information as **Confidential**.

5. **Secret and Top Secret**

Such information would be rarely encountered and expert advice **must** be sought as to its handling, storage and disposal.

HANDLING, STORAGE AND DISPOSAL PROCEDURES

Application/Activity	PROTECT	RESTRICTED	CONFIDENTIAL
Marking documents	Top and bottom of every page.	Top and bottom of every page.	Top and bottom of every page.
Storage and hard copy documents	Protected by one barrier, eg a locked container within a secure building.	Protected by one barrier, eg a locked container within a secure building.	Protected by two barriers, eg a locked container in a locked room, within a secure building.
Disposal of waste paper	Use secure waste sacks. Keep secure when left unattended.	Use secure waste sacks. Keep secure when left unattended.	Use a SEAP approved cross cut shredder. Keep secure when left unattended.
Disposal of magnetic media	Securely destroy. Floppy disk – dismantle and cut disk into quarters and dispose with normal waste. Optical media – destroy completely – disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.	Securely destroy. Floppy disk – dismantle and cut disk into quarters and dispose with normal waste. Optical media – destroy completely – disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.	Securely destroy. Floppy disk – dismantle and cut disk into quarters and dispose with normal waste. Optical media – destroy completely – disintegrate, pulverise, melt or shred. Use approved contractor for bulk items.
Reuse of media (hard drives, etc)	Triple overwrite using CESG approved software.	Triple overwrite using CESG approved software.	Triple overwrite using CESG approved software.

Application/Activity	PROTECT	RESTRICTED	CONFIDENTIAL
Movement within Force using own internal distribution system	In a sealed envelope with protective marking shown. A transit envelope may be used if sealed with a security label.	In a sealed envelope with protective marking shown. A transit envelope may be used if sealed with a security label.	In a new sealed envelope with protective marking shown. Transit envelopes must not be used.
Movement between forces/partner agencies	By post or courier, in a sealed envelope. Do not show protective marking on the envelope.	By post or courier, in a sealed envelope. Do not show protective marking on the envelope.	By post or courier. Double enveloped both fully addressed. Protective marking shown on inner envelope only. Return address on outer envelope.
Internal telephone network	May be used.	May be used if private secure network.	May be used if private secure network in cases of operational urgency.
Public telephone, mobile telephone and WAP telephone networks	May be used.	May be used in cases of operational urgency if due caution is exercised.	Not to be used.
Pager systems and SMS	May be used.	Not to be used.	Not to be used.
Facsimile machines	May be used.	May be used in cases of operational urgency if due caution is exercised.	Not to be used unless encrypted fax service available.

Application/Activity	PROTECT	RESTRICTED	CONFIDENTIAL
Airwave radios	May be used.	May be used.	Not to be used unless enhanced end to end encryption service deployed.
Force Data Network, email services using PNN – GSI – NHS – CJSM – MOD secure addressing conventions	May be used.	May be used.	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.
Internet email/internet services	May be used.	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.	Not to be used without encryption service compliant with ACPO/ACPOS Community Security Policy.