



## Data Protection Policy

The Office of the Police and Crime Commissioner (OPCC) is committed to the principles of equality and diversity. No member of the public, member of staff, volunteer or job applicant shall be discriminated against on the grounds of age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; or sexual orientation.

### Introduction

West Midlands Police and Crime Commissioner has a legal obligation to comply with the Data Protection Act 1998; this Act establishes standards and governs the processing of personal data. The Chief Executive is the Data Controller for the Office of the Police and Crime Commissioner (OPCC). The Data Protection Act 1998 regulates the use of information from which a living individual can be identified. It applies to the processing of personal data (including holding, collecting, receiving, viewing, transmitting). This policy outlines how the Data Protection Act applies to the OPCC and the responsibility of every employee of the OPCC.

### The Data Protection Act and Definitions

1. The Data Protection Act 1998 (the Act) imposes a set of rules on all organisations that collect, process and disclose personal data. For the purpose of the Act, personal data is defined as follows:

*Any information that may be used to identify a living individual, either from that data alone, or from that data and any other information held, or is likely to be held by the Data Controller. This includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual. This may include information on or in:-*

- *Computer records and printouts*
- *Emails – Including emails of a confidential nature specifically naming individuals*
- *Backup / archive systems*
- *Word-processed documents*
- *CCTV recordings*
- *Audio / Video recordings*
- *Microfiche*
- *Some card indices*
- *Some manual filing systems*
- *Notice Boards*
- *Radio Transmissions*
- *Personal files*
- *Social networking sites*
- *Internet / intranet*

## 2. **Data Subject**

An individual who is the subject of personal data

## 3. **Sensitive Personal Data** (which merits extra protection under the terms of the Act): Personal data consisting of information as to:

- an individual's racial or ethnic origin
- their political opinions
- their religious beliefs (or other similar beliefs)
- whether they are a member of a trade union
- their physical or mental health or condition
- their sexual life
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

## 4. **Data Processing**

Processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:

- Organising, adapting or altering the information or data
- Retrieval, consultation or use of the information or data (which, in relation to personal data, includes using the information contained in the data)
- Disclosure of the information or data (which in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available; or
- Alignment, combination, blocking, erasure or destruction of the information or data

## 5. **Data Controller**

A person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal information are, or are to be, processed. The Chief Executive is the Data Controller for the OPCC.

## **Data Protection Principles**

## 6. All personal data must be collected, processed, maintained and disclosed in accordance with the eight Data Protection Principles (Schedule One, Part One of The Data Protection Act), which specify that personal data must:

- (1) Be processed fairly and lawfully
- (2) Be processed for a specified purpose
- (3) Be adequate, relevant and not excessive
- (4) Be accurate and up to date
- (5) Not be kept longer than is necessary
- (6) Be processed in accordance with individual's rights
- (7) Be kept secure
- (8) Not be transferred to other countries without adequate protection

## **Notification**

7. The national body for the supervision of Data Protection is the Information Commissioners' Office (ICO) to whom the Chief Executive notifies his purposes for processing personal data.

This notification process serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the Data Protection Act 1998 that the public should know, or be able to find out who is carrying out the processing of personal data and for what purpose.

## **Related Policies**

8. For more information on how the OPCC manages information, please refer to the Information and Records Management Policy and also the Freedom of Information Policy. Both of these can be viewed on the Police and Crime Commissioner's website.

## **Roles and Responsibilities**

### **9. Data Controller**

The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes and manner for which any personal data are, or are to be, processed. The Chief Executive is the Data Controller for the OPCC.

### **10. All Managers**

It is the responsibility of all staff who have a supervisory role to ensure that their staff operate within the terms of the Data Protection Act and any associated policies and procedural guidance. This must include regular checks of work to identify training and development needs in this area and to ensure that the quality of information assets is of a high standard.

### **11. All Staff and Volunteers**

Every member of staff or volunteer working for or on behalf of the OPCC having access to personal data is required to comply with the requirements of the Data Protection Act and guidance contained in operating rules, conventions, policies and procedures for each system or business area designed to help achieve compliance.