WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Data Protection**
POLICY REFERENCE NO:	**Inf/03**

Executive Summary

West Midlands Police is committed to protecting the rights of individuals with regard to the processing of personal data. It will comply with, and process personal data in accordance with the provisions of the Data Protection Act 1998 in all respects.

***Any enquiries in relation to this policy should be made be made directly with that of the policy contact / department shown below.*

Intended Policy Audience

This policy applies to every police officer, member of police staff, police community support officer, special constable, volunteer, contractor, and approved persons working for or on behalf of West Midlands Police whether responsibilities include updating or simply using West Midlands Police information containing personal data.

Current Version And Effective Date.	**V.1.5**	**January 2015**
Business Area Owner	**Information Services**	
Department Responsible	**Information Management**	
Policy Contact	**Data Protection Manager**	
Policy Author	**Kate Firkins (51264)**	
Approved By	**Chief Information Officer – C Price**	
Policy Initial Implementation Date	**11/01/2013**	
Review Date	**12/01/2016**	
Protective Marking	**Not protectively marked**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- **ACPO Data Protection Manual of Guidance Part I: Standards v5.2**
- **ACPO Community Security Policy**
- **Guidance on the Management of Police Information (MoPI)**
- **Government Protective Marking Scheme**
- **Data Protection e-learning D-11**
- **Code of Ethics (**http://www.college.police.uk/docs/Code_of_Ethics.pdf**)**

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP database on the Intranet.

Force Diversity Vision Statement and Values

"Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values"

"All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay."

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organization to do the right thing.

CONTENTS

1. INTRODUCTION

1.1. West Midlands Police has a legal obligation to comply with the Data Protection Act 1998; this Act establishes standards and governs the processing of personal data.

1.2. The Chief Constable is the Data Controller for West Midlands Police. The Data Controller has appointed a Data Protection Manager to direct the day to day operation of the Act within West Midlands Police

1.3. 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).

1.4. This policy outlines:

- How the Data Protection Act applies to employees of West Midlands Police (and any person processing personal data on our behalf);
- The responsibility of every employee of West Midlands Police under the Act who processes personal data on behalf of West Midlands Police;
- Provides basic information about how to deal with disclosures; and
- Aids the compliance aspects of the ACPO/ACPOS Community Security Policy.

The Data Protection Act and Definitions

1.5. 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:

Personal Data (or information):

1.6. 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
- Pocket Note books
- 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

Data Subject:

1.7. An individual who is the subject of personal data

Sensitive Personal Data (which merits extra protection under the terms of the Act):

1.8. 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.

Data Processing:

1.9. Processing in relation to information or data, 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

Data Controller

1.10. 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 Constable is the Data Controller for West Midlands Police.

2.0 DATA PROTECTION PRINCIPLES

2.0.1 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

2.1 Notification

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

2.1.2 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.

2.2. Lawful Processing of Personal Data

2.2.1 The principal purpose for which West Midlands Police processes information is for a 'Policing Purpose' which is defined as:-

- Protecting life and property;
- Preserving order;
- Preventing the commission of offences;
- Bringing offenders to justice
- Any duty or responsibility arising from statute or common law

2.2.2 Data is also processed for specific purposes connected with the administration of the Force, its employees and the provision of necessary services to support the 'Policing Purpose'.

2.2.3 Access to information systems or personal data, including browsing, use or disclosure, is only permitted to employees, agents and approved persons working for or with West Midlands Police, where it is necessary in the course of their official duties for policing purposes and in accordance with Force policies and procedures.

2.2.4 Where a member of West Midlands Police is involved in or witnesses a crime or incident whilst off duty, no access to the recorded information can be made without prior authorisation from their supervisor.

2.2.5 Access to any force ICT equipment must be controlled. Only authorised users in the course of official police business should have access.

2.2.6 The use of police information systems for a private purpose or any other purpose other than that declared by the Chief Constable to the Information Commissioner is strictly prohibited.

2.2.7 It is NOT acceptable for a member of West Midlands Police to conduct checks on:

- Nominal's living in close proximity to them / family / friends;
- Friends or friends of family members;
- Prospective employees of friends or family;
- Individual applying for membership of social / other clubs;
- The desirability of property;
- Individuals subject to enquiries by private detective agencies.
- Celebrities or high profile arrests

This list is not exhaustive.

2.2.8 Deliberate unauthorised access to, copying, destruction and/or alteration of, or interference with any computer or ancillary equipment or data (soft or hard copy) is also strictly prohibited.

2.2.9 In order to meet the requirements for lawful processing, particular consideration will be given to:-

a) Confidentiality arising from the relationship between West Midlands Police and any individual;
b) The ultra vires rule and the rule relating to the excess of delegated powers, under which officers may only act within the limits of their legal powers;
c) The legitimate expectations of any individuals in relation to the processing of information about them; and
d) Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence).

2.3. Fair Processing

2.3.1 In meeting any obligation to ensure that processing of information is fair, due consideration will be given to the adoption of any recognised standards or advice to provide individuals with such information as is necessary to ensure that they are likely to understand:-

a) the purposes for which their personal data are to be processed;
b) the likely consequences of such processing and;
c) whether particular disclosures can be reasonably envisaged

2.3.2 Staff collecting information about individuals will, wherever possible, give a brief explanation as to what their information may be used for. Individuals should also be told if their information is likely to be passed to a third party.

2.4. Disclosure of Personal Data

2.4.1 Disclosure of information may take many forms, including viewing records on a terminal, computer printouts, typewritten material, by word of mouth or radio transmission including telephone and Airwave.

2.4.2 Information from police systems will, in the first instance, only be disclosed to serving officers or other police personnel who require such information in order to carry out their official duties.

2.4.3 Requests for the disclosure of any personal data will only be considered once the member of staff is fully satisfied that the requestor is authorised to receive the information.

2.4.4 Care will be taken to ensure that any disclosure is within that allowed by any prevailing policy, guidance, Information Sharing Agreement, Memorandum of Understanding or statutory obligation and is authorised at the appropriate level.

2.4.5 Further specific advice and guidance concerning any aspect of information sharing or disclosure may be obtained from the Data Protection Unit or the Information Commissioners' website.

2.5. Police Enquiries – Access to personal data held by other organisations

2.5.1 Sometimes it is necessary to seek information relevant to a police enquiry from other organisations (credit details, bank details, medical details etc)

2.5.2 In these circumstances, the organisation receiving the police enquiry may request a Section 29(3) Disclosure of Information Form (Force Standard Form WA170) stating the reason and what specific information is sought.

2.5.3 The exemption to the rules of non-disclosure, which is most likely to affect police officers, provides that personal data is exempt from the non-disclosure provisions of the Act in cases where the disclosure is for any of the following purposes:-

- the prevention and detection of crime
- the apprehension or prosecution of offenders

2.5.4 These exemptions only apply to the extent that if the data were not disclosed to the police it would be likely to prejudice police investigations.

2.5.5 It should be noted that although we are able to use Section 29(3) of the Data Protection Act for legitimate police enquiries it is still a matter for the organisation to determine whether or not to disclose the information as there is no element of compulsion in this respect.

2.5.6 For audit purposes, a copy of the request is to be kept with the associated crime papers.

2.5.7 If an Information Sharing Agreement is in existence the rules of that agreement should be followed.

Where disclosure is in the vital interest of the data subject

2.5.8 There are provisions under the Data Protection Act 1998 which cater for circumstances where there is a genuine life or death situation (severe medical emergency or a potential suicide for example) and where the usual approach for a disclosure is not possible.

2.5.9 These provisions are contained within Schedules 2 & 3 of the Data Protection Act and refer to the Vital Interests of the data subject.

2.5.10 Officers making use of this process should ensure that the events are adequately documented and retained pending any future challenge over possible unlawful processing of personal data.

Use of Section 29(3) exemption by other organisations

2.5.11 Other organisations may also request information from the police under the non-disclosure exemption provided by Section 29(3). Normally such use will be by organisations that have the ability to investigate and/or prosecute offences.

2.5.12 It should be noted that there is no obligation for West Midlands Police to comply with such a request and any disclosure must only be made in accordance with relevant Force policies and/or prevailing legislation.

2.5.13 Each request should be considered on its individual merits and disclosures made only where the relevant considerations are satisfied. The receipt of such requests together with the decision and any relevant responses should be recorded and retained on the appropriate file and available for any future audit or inspection.

2.6. Adequacy and Relevance of Data

2.6.1 The reliability of information held in police information systems depends primarily on the professional competence of police officers and staff who obtain and record information.

2.6.2 Information held on police systems must be adequate i.e. fit for purpose, unambiguous and professionally worded. All abbreviations, warning signals and information markers must comply with national standards.

2.6.3 Forms designed for the collection of information should only record that information which is pre-determined to be relevant in relation to the purpose for which it is required.

2.6.4 Criminal intelligence will be graded using the 5x5x5 evaluation system in accordance with the National Intelligence Model and Management of Police Information (MoPI) standards, which gives an indication of the quality of the information and the reliability of the source.

2.7 Accuracy of Data

2.7.1 It is the responsibility of the person who receives the original information to ensure, as far as is possible, that it is accurate, valid and up-to-date.

2.7.2 All staff will ensure wherever possible, that all information entered on police records is adequate, relevant, unambiguous and professionally worded. Where errors are found on any personal data held they will be reported to a supervisory officer and corrected at the earliest opportunity.

2.7.3 Cancellations, amendments and deletions will be carried out as a matter of priority.

2.7.4 The source of information received from an individual or from a third party will be recorded accurately. Notations of this nature will assist into any investigation, should the information or its source be challenged.

2.7.5 Where it is known that inaccurate information may have been disclosed to a third party, the corrected information will be disclosed to that party with explanation, together with any other action necessary to minimize any harm, loss or damage arising from such disclosure.

2.8. Review, Retention and Disposal of Data

2.8.1 Unless a system incorporates automatic facilities or other structured procedures, reviews of personal data must be carried out at frequent intervals to ensure immediate cancellation or amendment of unwanted or out-of-date material. This is good practice that should be applied to all information held.

2.8.2 Current procedures on the MoPI Review, Retention and Disposal (RRD) Policy and other legal requirements for the retention of documents should be referred to for further guidance on this subject.

Exceptional Case Review

2.8.3 The processing of requests for the deletion of PNC records, fingerprints and DNA samples will be carried out in accordance with the advice and guidance provided by the ACPO Criminal Records Office (ACRO) and will be managed by the Data Protection Unit.

3.0 SUBJECT ACCESS

3.1. Under Section 7 of the Data Protection Act every individual has the right of access to their personal data. The force Subject Access policy and procedure is available separately.

3.2. As previously stated, the Information Commissioner is the body that oversees compliance with the Data Protection Act 1998. Where a data subject is unhappy with some aspect of the processing of their personal data, or a disclosure they have or have not received from the Force, they have the right of appeal to the Information Commissioner.

3.3. Any request for an assessment or correspondence from the Information Commissioner should be responded to promptly and co-ordinated through the Data Protection Manager.

4.0 FREEDOM OF INFORMATION ACT 2000 (FOI)

4.1. The FOI Act extended the provisions of the rights given under the Data Protection Act for individuals to request information held by any public sector organisations. The effect of those changes is that (subject to certain exemptions) the subject access and FOI provisions now cover most forms of information held by the Police, including computer, manual records and other media.

4.2. FOI enables any individual to request information from any UK Public Sector organisation. The FOI policy and procedure is available separately.

5.0. INFORMATION SECURITY

5.1. Principle 7 of the Data Protection Act 1998 requires that appropriate technical and organisational measures shall be taken to protect data against:

- Unauthorised access;
- Unauthorised or unlawful processing;
- Accidental loss, destruction or damage

5.2. Appropriate technical and organisational security measures will include:

a) using and developing technological solutions to ensure compliance with the data protection principles
b) using and developing physical measures to protect Force assets
c) ensuring the reliability of any persons who have access to police information
d) reporting and investigating security breaches

5.3. These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction or damage. The Government Protective Marking Scheme (GPMS) provides for such considerations and is adopted by West Midlands Police as part of its compliance with the ACPO Community Security Policy.

5.4. All printout material, magnetic tape, diskettes, CD's or DVD's, manual files, hand written notes etc. which contain personal data and are no longer required, will be treated as confidential waste and disposed of securely

5.5. Where processing of police data is to be carried out by a third party on behalf of the Force, the Chief Constable must ensure that the third party provides sufficient guarantees in respect of the technical and organisation measures governing

5.6. the processing to be undertaken. This means that appropriate contractual terms and conditions will be imposed on any third party data processor to ensure that they act only on instructions given by the Chief Constable in regard to that processing.

5.7. In those circumstances where West Midlands Police use the services of a third party processor but there are no financial or procurement considerations, advice will be sought from the Data Protection Manager to ensure the Chief Constables' responsibilities under the Act are fulfilled.

5.8. Good information security is also achieved through policy and procedural controls. For further guidance please refer to:-

- Force Vetting Policy
- Force Information Security Policy (FISP)
- Government Protective Marking Scheme (GPMS)
- Email Security Policy
- Internet / Intranet Security Policy
- Records Management Policy
- Police National Computer Policy
- Information Disclosure Policy
- Information Sharing Agreement Policy
- Information Management Strategy
- Social Networking Policy
- FOI Policy
- Confidential / Secure Waste Policy

5.9. In accordance with the Force Information Security Policy all members of the Force should note and report any breach of information security or suspected security weakness as quickly as possible through line management channels to the Information Security Officer. Under no circumstances should users attempt to prove a suspected weakness.

5.1 Audit and Monitoring

5.1.1 In order to ensure compliance with the Data Protection Act 1998, the Code of Practice on the Management of Police Information and other relevant standards for the management of police information, the Chief Constable is obliged to have an audit regime to measure performance to comply with legislative and policy requirements and thereby help in endorsing the effectiveness and efficiency of operational policy.

5.1.2 The purpose of the Audit is to provide a systematic and independent examination to determine whether activities involving the processing of police information are carried out in accordance with the organisation's policies and procedures and whether this processing meets the requirements of relevant legislation and standards.

5.1.3 The Force Record Manager will develop a Strategic Audit Programme and annual plan from comprehensive risk analysis in accordance with the framework and standards provided by the ACPO Data Protection Manual of Guidance Part II; Audit and the Home Office.

5.1.4 This will determine the nature and scope of the audit, taking into account available resources and provide a strategy which will form the basis of audit activity for the period under consideration. This Strategy will be subject to annual review and lead to a documented Strategic Audit Plan which will outline:

- Areas to be audited;
- Target dates and;
- Resource allocation

5.1.5 It is recognised that limited resources may restrict the number of applications or systems, which may be audited. However, the decision regarding which applications or systems will be audited and the scope and frequency of such audit will be subject to a formal risk assessment process and current business needs.

5.1.6 The Strategic Audit Programme and annual plan will be subject to review and approval by the Strategic Information Board chaired by the Chief Information Officer. The Plan and associated risk analysis documentation will be available for inspection by external auditors as required.

5.1.7 Individual audits (as specified in the Strategic Audit Programme) will be subject to a separate planning process, with the aim of performing the audit in an effective and efficient manner. The audit plan will set out the follow:

- The scope and objectives of the audit;
- Conduct/methodology (e.g. sample size, sample selection) of the audit;
- Audit programme (detailing error classification and audit tests to be carried out);
- Resource allocation and target timescales

5.1.8 The Audit programme will be supplemented by quality assurance and monitoring processes undertaken by supervisors and managers in each business area.

5.1.9 Transaction checks will also be carried out on a regular basis in order to:-

- Deter and detect unauthorised access to police information or systems;
- To raise staff awareness of data protection issues and maintain public confidence in the use of police information and
- To ensure that all required transaction fields are completed to provide an adequate audit trail for retrospective investigations into transactions that have been carried out.

5.2 Legislative Requirements/National Guidance/Policy Requirement

5.2.1 West Midlands Police recognises that personal data is a primary asset to the Force. The legal basis for this policy is the Data Protection Act 1998 which provides the legal parameters for the processing of personal data.

5.2.2 However, compliance with other legislation, Codes of Practice, policies and guidance also has relevance, such as:

- The Freedom of Information Act 2000
- The Computer Misuse Act 1990
- The Copyright, Designs and Patents Act 1988
- The Official Secrets Acts and
- The Code of Practice on the Management of Police Information
- The Crime and Disorder Act 1998
- Human Rights Act 1998
- Rehabilitation of Offenders Act 1974
- ACPO Data Protection Manual of Guidance

5.2.3 All systems must also comply with the relevant ACPO policy including:-

- ACPO Community Security Policy
- Police National Standard Operating Rules applicable to all Police computer applications.

5.3. Criminal Offences, Liability and Compliance

5.3.1 There are a number of criminal offences contained within the Data Protection Act 1998. The Data Controller is guilty of an offence if they:

- Are processing without notification;
- Fail to notify the Commissioner of changes required to update the notification register entry;
- Fail to comply with written requests for particulars;
- Fail to comply with an enforcement notice/information notice/special information notice;
- Knowingly or recklessly make a false statement in compliance with an enforcement notice or special information notice;
- Intentionally obstruct, or fail to give reasonable assistance in the execution of a warrant.

5.3.2 All employees of West Midlands Police can be personally criminally liable if they disclose or obtain personal data without the authority of the Data Controller. To make, or encourage another person to make an unauthorised disclosure knowingly or recklessly may result in criminal liability. The offences that apply are Section 55 of the Data Protection Act and are as follows:-

a) Without the consent of the Data Controller, knowingly or recklessly to unlawfully obtain or disclose personal data or the information contained in personal data.

b) Without the consent of the Data Controller to knowingly or recklessly procure the disclosure to another person of the information contained in personal data.

5.3.3 It is also an offence for any person to sell personal data if it has been obtained in contravention of the above.

5.3.4 Examples of relevant activities that may amount to an offence include, but are not limited to:

- Browse 999 calls/other information for personal interest/out of curiosity;
- Access crime or intelligence nominal records/other information to check the progress of a family matter, advise a concerned relative of their partner's background, check their daughter's new boyfriend's history;
- Disclose information to a friend who works for a partner agency and is seeking information about an individual (without going through the designated Information Sharing Agreement/procedures);
- Offer to sell police intelligence to a member of a criminal gang;
- Remove confidential waste/computer printouts to show family members;
- Obtain personal data using the s29(3) exemption form to obtain bank details for own purposes.

Monetary Penalty Notice

5.3.5 Under sections 55A and 55B of the Data Protection Act 1998 introduced by the Criminal Justice and Immigration Act 2008, the ICO may, in certain circumstances, serve a monetary penalty notice on a data controller.

5.3.6 A monetary penalty notice is a notice requiring a data controller to pay a monetary penalty of an amount determined by the ICO and specified in the notice. The amount of the monetary penalty determined by the ICO can not exceed £500,000.

5.3.7 The ICO may impose a monetary penalty notice if a data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

Other Relevant Offences

5.3.8 It should be noted that the misuse of official personal data can also be dealt with as an offence of '**Misconduct in Public Office'**, which can attract a custodial sentence.

5.3.9 The **Computer Misuse Act** also contains offences relating to the unauthorised access to information (not limited to personal data) and includes accessing information held in systems that the offender has authorised access to for official purposes, but where the access on the relevant occasion was unauthorised.

5.3.10 In addition, **the Freedom of Information Act 2000** creates the following offence in relation to personal data:

Section 77: Altering, defacing, blocking, erasing, or concealing any record to prevent disclosure under Section 7 of the Act which refers to Subject Access.

5.4. Breaches of the Data Protection Act.

5.4.1 All breaches or suspected breaches of the Data Protection Act 1998 must be reported promptly to the Professional Standards Department.

5.4.2 The ACPO Data Protection Manual of Guidance sets out the procedures for the recording and handling of allegations of criminal offences committed in contravention of the Data Protection Act 1998. It describes the role of the police and the ICO and the actions to be taken when criminal offences under the Act are suspected.

5.5 Roles and Responsibilities

5.5.1 **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 Constable is the Data Controller for West Midlands Police.

5.5.2 **Data Protection Manager**
Within West Midlands Police, this is an appointed police staff member within Information Services and is responsible for managing the Chief Constable's statutory obligations in respect of the Data Protection Act inclusive of the notification to the Information Commissioner of the processing of personal information

5.5.3 **All Managers/Supervisors:**
It is the responsibility of all Officers and staff who have a supervisory role to ensure that their staff operate within the terms of the Data Protection Act and any associated Force 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 Force information assets is of a high standard.

5.5.4 **All Staff**
Every police officer, member of police staff, police community support officer, special constable, volunteer, data processor, contractor and approved persons working for or on behalf of West Midlands Police 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.

6. EQUALITY IMPACT ASSESSMENT (EQIA).

6.1. The Policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how WMP has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this Policy.

7. HUMAN RIGHTS

7.1 This policy has been implemented and reviewed in accordance with that set out with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of WMP (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

8. FREEDOM OF INFORMATION (FOI)

8.1 Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 1.5 of this policy has been GPMS marked as not protectively marked.

8.2 Public disclosure does not automatically apply to supporting Force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number
n/a		

9. TRAINING

9.1. Successful completion of the on-line NCALT training 'Lawful Handling of Information' is a pre-requisite to obtain access to force systems including obtaining an email account.

9.2. This training is an introduction to the Data Protection Act, the Freedom of Information Act and to Information Assurance (including the GPMS). It is designed to assist police officers and staff to meet their responsibilities with regards to the information contained within police systems.

9.3. The course is an on-line, self-teach programme, delivered via NCALT and can be accessed from any terminal connected to the Intranet, anywhere in the force, at any time of day.

9.4. All details of training commenced, progress, and completion are held centrally and accessible by the Data Protection Manager.

9.5. Non-completion will result in the individual being denied access to the force network and all systems until the training is completed. In this event, the individuals line manager / supervisor should assess the risk of leaving the individual in any role with unsupervised access to personal data and take action accordingly.

9.6. Individuals who re-join the force in a new role i.e. as a special constable; or who have had a break in service of more than 6 months, or are returning from long term sick are required to repeat the training.

9.7. All Managers and supervisors should encourage individuals to refresh their knowledge of data protection and the requirements the Act places upon them at every opportunity.

10. PROMOTION / DISTRIBUTION & MARKETING

10.1. The following methods will be adopted to ensure full knowledge of the Policy:
Details of this policy will be available on the force Intranet within the force policy portal and specific guidance available from the Data protection Unit, Information Services.

11. REVIEW

11.1 The Policy business owner maintains outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

11.2 The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

11.3 A formal review of the Policy document, including that of any other potential impacts i.e. EQIA, will be conducted by the date shown as indicated on the first page.

11.4 Any amendments to the Policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

11.5 Feedback is always welcomed by that of the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.

CHIEF CONSTABLE

12. VERSION HISTORY

Version	Date	Reason for Change	Amended/Agreed by.
1.1	05/09/12	Policy Review (supersedes Part 1 order 14/2000)	51264 Firkins
1.2	18/09/12	Presentation amendments	4566 Brookes
1.3	03/01/2013	To Command Team for approval	Mr Chris Price
1.4	11.01.2013	To CC for authorisation	CC Chris Sims
1.5	12/01/2015	Review; section 9 updated to include Lawful of Handling Information training.	51264 Firkins
1.5	13/01/2015	Formatting adjusted before publication, Standard Code of Ethics section included	56408 Couchman