STANDARD OPERATING PROCEDURES:
OFFICE OF THE BEDFORDSHIRE POLICE AND CRIME COMMISSIONER

Title	Data Protection Policy
Area of Compliance	Business and Compliance
SRR Ref. No.	PCC – SR8
SOP Ref. No.	010/2015
Version No.	Version 1.0
Senior Lead	Chief Executive
Author	Compliance Officer

Revision History

Date	Revision	Change	Section	Review Date
December 2015	1.0	New Document		

1. Purpose

The purpose of this document is to ensure compliance against the Data Protection Act (DPA) 1998. The DPA places obligations on employers in regard to personal information (data) which they process about any living individual. The purpose of the Act is to protect the privacy of individuals. The Act covers all personal information held both about the public and about Police & Crime Commissioner employees.

Under the DPA, every individual has a right of access to information that the Police & Crime Commissioner holds about him or her. This is known as the Subject Access right. When a Subject Access request is received, the information must normally be provided to the individual within 40 days.

By adhering to this document the OPPC will be complaint with the Data Protection Act (DPA) 1998.

2. Background

The DPA applies to all personal data held in any form e.g. paper, electronic, CCTV and photographs. Even where the data does not identify an employee by name the provisions of the DPA may still apply if the employee can be identified from other information held by the OPCC e.g. NI number.

The following eight principles apply to all personal data covered by the DPA 1998.

1. Personal data shall be processed fairly and lawfully

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall be processed in an appropriate manner for that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date. Your personal data will need to be updated from time to time.

5. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subject under this Act.

7. Appropriate security measures shall be taken against unauthorised access to or alteration, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

8. Personal data shall not be transferred without consent to a country or territory outside the EEA unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Employees of the Office of the Police & Crime Commissioner must adhere to the Data Protection principles when they deal with personal data in the course of their work.

3. Affected persons

This policy will apply to all staff working in the Office Police & Crime Commissioner (OPCC) whether employed full-time or part-time, fixed term, permanent, seconded or on a temporary basis.

4. Strategic Risk Register

The Data Protection Policy will be monitored within the Strategic Risk Register to ensure full adherence to the policy at all times.

5. Policy

When a Subject Access request is received, employees should inform the Chief Executive and in their absence a senior member of the OPPC Team.

Employees should be aware of any problems that occur with the security, accuracy or disclosure of information that may compromise the Police & Crime Commissioner's duty to adhere to the Act. Concerns should be brought to the attention of the Chief Executive and in their absence a senior member of the OPPC Team.

Employees consent to the Police & Crime Commissioner processing their personal data (including sensitive personal data relating to their health, trade union membership and racial or ethnic origins) for the purposes of the administration and manager of the OPCC and its employees and to ensure compliance with any applicable laws, regulations and procedures. Employees also consent to the Police & Crime Commissioner making such data available to persons other than the Police & Crime Commissioner where it considers this necessary or in the interests of the Police & Crime Commissioner.

Employees may request to see personal data held by the Police & Crime Commissioner, including their personnel files, subject to the legal and regulatory requirements and provisions of the DPA. There is a nominal fee (currently £10) in respect of each such request and the Office & HR Manager will endeavour to supply this information as soon as possible and within the 40 day time period anticipated in the DPA.

Vetting Procedure

It is important operationally, legally and for public confidence, that we should ensure that employees have integrity and therefore the Office of the Police & Crime Commissioner follows a vetting procedure. Once fully implemented, the public, and other organisations may be confident that the office team have been appropriately examined:

- In relation to criminal behaviour
- In relation to National Security
- In relation to integrity

All employees allowed access to police information or assets will follow the instructions contained in the Force Vetting Procedure. Failure to conform to those instructions may result in a vetting refusal, disciplinary, or criminal action.

It will be the responsibility of the subject and their Line Manager to report to the Force Vetting Officer all matters which may affect the vetting status of their employees at the earliest opportunity.

For further information regarding the Police & Crime Commissioner's vetting procedure please refer to Recruitment, Selection, Posting and Promotion Policy.

Freedom of Information Act 2000

The Freedom of Information Act 2000 (FOIA) gives a general right of access to information that is held by public bodies. This right of access applies to anyone or any organisation, anywhere in the world. The Police & Crime Commissioner has two main duties under the FOIA:

1. To produce a publication scheme: Such schemes provide the framework within which significant amounts of public information can be made routinely available, without the need for individuals to request it specifically. The scheme must be kept up to date and new information should be added to it as it becomes available.

2. From 1 January 2005 the Act will cover written requests for information made to the Police & Crime Commissioner. Requests may be made by any person or organisation and must be answered within 20 working days. The applicant must be informed of whether the information is held by the Police & Crime Commissioner and, if so, the information should be supplied to them, unless one of the exemptions available under the Act applies.

For further information regarding Freedom of information please refer to the Freedom of Information Policy.

Information Security

The Police & Crime Commissioner will take appropriate and proportionate measures to protect personal data held in the organisation from unauthorised access, theft, misuse and alteration. This will include:

- Controlling access to Police & Crime Commissioner's premises and computer equipment
- Ensuring the protection of electronic systems
- Restricting staff access to those who require personal data for their work.

The purpose of the policy is to protect the business of the constabulary by protecting the confidentiality, integrity and availability of information, and by providing evidence of trustworthiness in information sharing arrangements. More specifically the policy is intended to:

- minimise the impact of security breaches
- reduce or avoid threats
- reduce vulnerabilities
- detect the occurrence of security breaches
- Recover from security breaches.

The Police & Crime Commissioner recognises that Internet facilities (including internal e-mail, internet, e-mail, web browsing and web site) offer considerable benefits for employees. The Office to the Police and Crime Commissioner ensures that the internet system maintains the appropriate levels of security, confidentiality, integrity and access to the Constabulary's data and information.

Data Breaches

- Any incident that could or does lead to loss, disclosure or temporary exposure of personal information must be reported to the Monitoring Officer in accordance with the OPCC's incident management procedures.

- The OPCC has procedures for investigating data protection and privacy breaches and all those affected will be expected to co-operate with any such investigation. The OPCC may be required to report serious data protection breaches to the Information Commissioner's Office or other regulatory bodies.

- Disregard for the OPCC's data protection and related policies by employees may be regarded as misconduct to which the OPCC's dismissal and disciplinary procedures shall apply and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal. In the case of contractors, representatives, workers and volunteers, this may be grounds for termination of that relationship with the OPCC.

Information Responsibilities for Staff

All staff will be responsible for managing the information they create, receive, hold, and transmit. Staff must:

- Know what information you are responsible for;
- Make sure you achieve high standards of accuracy and quality when creating and recording any information;
- Keep the information up-to-date;
- Classify and protect information according to its sensitivity, value, and importance;
- Understand how information should be handled, who should receive or have access to it;
- Make sure the information is secured, both physically and electronically;
- Keep information for no longer than necessary – use agreed retention and disposal schedules applicable to your information;

- Respect people's rights to privacy and confidentiality, and to access to their own personal information;
- Respect people's right to access information that the OPCC creates, owns or holds and assist them in accessing it;
- Make the best use of information to deliver and improve services;
- Report any security incidents, potential or actual losses of information or equipment to your line manager and the Monitoring Officer;
- Understand and adhere to the OPCC's information governance policies and procedures;
- Seek advice and guidance whenever you need it from your line manager or the Monitoring Officer;
- The Information Commissioner's Office has the responsibility for making sure organisations comply with information legislation and issues good practice which we incorporate into our policies and procedures. Failure by the OPCC to comply with legislation and good practice may lead to enforcement and improvement measures, possible fines and loss of reputation. There are also penalties for individuals in the most serious circumstances; and
- For any member of staff, disregard of these responsibilities may be regarded as misconduct, to which the OPCC's dismissal and disciplinary procedures shall apply. A serious breach of any policy may be treated as gross misconduct and may lead to dismissal

For further information please refer to the Force's policy - M006 Data Protection Procedure - designed to achieve appropriate protection for information whether held on paper or electronically, whether corporate or operational, and including evidence.

6. Responsibilities

Responsibility for ensuring the effective implementation and operation of the arrangements will rest with the Business and Compliance Manager. Managers will ensure that they and their staff operate within this policy and arrangements, and that all reasonable and practical steps are taken to avoid discrimination. Each manager will ensure that:

- all their staff are aware of the policy and the arrangements, and the reasons for the policy

Policy Statement

The Office of the Police and Crime Commissioner fully understands its obligations to ensure that personal information is processed lawfully and is committed to protecting the rights of individuals with regard to the processing and sharing of personal data.

The public must have confidence in the ability of the Office of the Police and Crime Commissioner to protect the confidentiality of personal data that it holds. The damage done to the reputation of the organisation by staff who are found to have committed a breach by unlawfully accessing, disclosing, holding or processing personal data cannot be overstated and this detracts from the credibility of the organisation. Consequently disciplinary action will be taken against staff failing to comply with this policy.

The Office of the Police and Crime Commissioner is committed to ensuring that staff are appropriately trained and supported to achieve compliance with the Data Protection Act.

It fully endorses and will adhere to the Data Protection Principles summarised below:-
Personal data must be:

- fairly and lawfully processed;
- processed for limited and lawful purposes;
- adequate, relevant and not excessive;
- accurate and where necessary kept up-to-date;
- kept for no longer than is necessary;
- processed in accordance with the rights of the data subject;
- kept secure;
- transferred only to countries with adequate security.