Philip Seccombe
Police and Crime Commissioner
for Warwickshire

DATA PROTECTION POLICY

Office of the Police and Crime Commissioner for Warwickshire

Policy/Procedure Title	**Data Protection Policy**
Responsible Party	

Security Classification	**NOT PROTECTIVELY MARKED**
Disclosable under Freedom of Information Act 2000	Yes

Policy Implementation Date	
Next Review Date Prior To	

Revision record

Date	Nature of revision
n/a	n/a

Introduction

The Data Protection Act 1998 ('DPA') requires the Office of the Police and Crime Commissioner for Warwickshire ('OPCC') to handle personal information relating to living identifiable individuals in a safe, responsible and secure manner. This policy sets out the OPCC's requirements regarding the appropriate and responsible use of personal information. It is underpinned by a number of related policies, codes of practice and guidelines.

The DPA and other legal requirements governing the use of personal information attempt to strike a balance between the privacy rights of individuals and the legitimate interests of other parties who need to access that personal information for specified purposes. The OPCC deals with individuals' personal information, in all sorts of formats, much of which is very private. The OPCC expects everyone who works on its behalf to recognise their responsibility for treating personal information with the care and respect it deserves.

The effect of a data breach can be very distressing and damaging to the individual concerned, and can also be damaging for the party responsible for the breach. The law does not create unreasonable barriers to the use of personal information. What the law does do is to create significant sanctions against individuals and organisations for unfair, unlawful, disproportionate, or reckless use of personal data.

The OPCC processes information in order to carry out its statutory duties. This may include confidential information about businesses and individuals, which is protectively marked.

Information, and the systems which support it, are vitally important to the OPCC's assets. Their availability, integrity, security and confidentiality are essential to maintain service levels, legal compliance and the image and perception of the OPCC. Threats to information security are becoming more widespread, ambitious and increasingly more sophisticated and the OPCC must maintain a policy to reflect this ever-changing environment.

Effective information security will help to control and secure information from inadvertent or malicious changes and deletions or unauthorised disclosure. The OPCC is committed to the secure use of information and information technology systems in order to protect the availability, integrity and confidentiality of the information under its control. The OPCC undertakes to have in place procedures to inform employees and to protect the information under its control from security breaches that might have an adverse impact on the OPCC's reputation.

Security problems can include confidentiality (the wrong people obtaining information), integrity (information being altered without permission, whether deliberate or accidental) and availability (information not being available when it is required).

Scope

This policy applies to:

- all employees
- all workers who are not employees (e.g. individuals supplied through an agency or other company or partner or subsidiary organisations, contractors, individuals seconded to the OPCC or otherwise engaged on the OPCC's business)
- all volunteers and any individuals on work experience at the OPCC's office

Any reference in this document to "employee" is deemed to be a reference to any of the above.

Policy Requirements

There are a number of OPCC requirements under this policy:

- The Data Protection and Privacy Commitment
- The Data Protection Act Principles
- Other policies and guidance on the use of personal information

Data Protection and Privacy Commitment

The OPCC has made a Data Protection and Privacy Commitment which explains the approach taken by the OPCC to comply with the DPA, the Human Rights Act 1998, the duty of confidence and other legislation and best practice relating to the use of personal information. Everyone to whom this policy applies is required to meet the Data Protection and Privacy Commitment.

The OPCC will seek to meet its obligations in law and in spirit and achieve an appropriate balance between the OPCC's resources, confidentiality, other people's rights to privacy and the purposes for which the information is held by doing the following:

1. Being transparent and fair in the way that the OPCC meets its legal obligations recognising the rights to privacy of individuals;
2. valuing the personal information entrusted to us and make sure we respect that trust;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems or new ways of working;
4. ensuring information held about individuals is accurate, relevant and subject to clear archiving and destruction policies;
5. ensuring that there are proper security measures in place to protect the confidentiality of individuals;
6. obtaining written, informed consent to collect, share and process personal information wherever reasonably practicable;
7. informing citizens what information we collect and share about them;

8. ensuring that personal information is used in ways which are proportionate and not excessive or unreasonable;
9. facilitating access to information where this does not prejudice the purpose for which the information is held or infringe rights to privacy;
10. maintaining up to date data protection registration with the Information Commissioner's Office;
11. treating people justly and fairly whatever their age, religion or belief, disability, gender, sexual orientation or ethnicity when dealing with requests for information;
12. raising awareness through effective staff training and induction;
13. treating it as a disciplinary matter if employees misuse or do not look after personal information properly;
14. setting out clear procedures for responding to information request; and
15. setting out clear procedures for making a complaint and ensuring a prompt response.

Data Protection Principles

The DPA sets out eight data protection principles to secure the responsible use of personal information.

All employees must comply with these principles and the OPCC's policies and guidelines that underpin them, which state that an individual's personal information should be:

1. Processed fairly and lawfully
2. Obtained for one or more specified and lawful purposes, and will only be further processed in compatible manner
3. Adequate, relevant and not excessive for the purposes
4. Accurate and where necessary kept up to date
5. Not kept for longer than is necessary for the purposes
6. Processed in line with the individual's rights
7. Appropriate technical and organisation measures to keep secure
8. Not transferred to other countries outside the European Economic Area without adequate protection.

The data protection principles also make it clear that personal information which is particularly sensitive (for example, information which relates to an individual's racial or ethnic origin, health, religion or belief, sexual life, trade union membership, political affiliations or criminal offences or proceedings) must be treated with special care. Information which is subject to a "duty of confidence" must also be treated with special care.

Information Governance Policies and Guidance

To assist the OPCC and its employees comply with its Data Protection and Privacy Commitment and the data protection principles, the OPCC has developed a number of other policies and guidance relating to personal information, data protection and privacy, which include:

1. Information management procedures
2. Information security procedures
3. Data protection and privacy procedures
4. Information responsibilities for staff
5. Access to information procedures
6. Information sharing protocols with other agencies, as appropriate
7. Codes of Conduct for employees
8. Any other instructions, guidance and controls issued by managers from time to time

Application and Management

All employees and any other person to whom this policy applies to are responsible for the appropriate use and protection of personal information which is in their possession or use. Everyone is also responsible for familiarising themselves with their obligations under this policy and related ones, for ensuring their own compliance and for seeking guidance where they need it.

Managers are responsible for controls that ensure compliance with this policy. This will include an induction for new staff, implementation of new procedures and systems and providing appropriate communications and raising awareness of the policy requirements.

The OPCC will designate the Monitoring Officer who will be responsible for coordinating and supporting staff on data protection and privacy policy and procedures.

The Monitoring Officer will act as the Senior Information Risk Owner (SIRO) for the OPCC ensuring that information risks are make a business priority at board level.

The Chief Executive is responsible for the information assets under the OPCC's control including personal information. This includes identification, access, risk management, security, and privacy of personal information. The Chief Executive shall ensure that employees who access or handle personal information are suitably trained in data protection and privacy in order to understand their obligations under this policy, and that an assessment of data protection and privacy risk is incorporated into risk management arrangements.

The Chief Executive is also responsible for ensuring a coordinated response from the OPCC and its employees to this policy, keeping under review the OPCC's approach to personal information, data protection and privacy, and ensuring that sufficient resources are made available to support its employees in meeting their obligations under this policy.

The Monitoring Officer shall be responsible for liaison with the Information Commissioner's Office over data protection notifications and other issues as appropriate.

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 Security Policy Statement

The OPCC's activities are critically dependent on information and information systems. Consequently, the OPCC has a continual commitment to protect OPCC and stakeholder information. The application of information security across the OPCC is founded upon the following guiding principles:

1. Information is a critical asset and all storage, transmission, and processing of information in the possession of, or under the control of the OPCC should only be carried out for the purposes for which it is held and in respect of sensitive information should only be carried out for the purposes expressly authorised by senior management;
2. Information will be classified and protected in a manner commensurate with its sensitivity, value, and criticality;
3. Information will be protected from loss of confidentiality, integrity and availability;
4. Information that is classified as restricted and in the possession of, or under the control of the OPCC should only be provided on a need to know basis and disclosed only to those people who have a legitimate need for that information;
5. Information security requirements will be identified by assessment of risks to determine the balance of investment in information security against the risk to the OPCC and its stakeholders;
6. A process of continual review and improvement will be implemented;
7. Users, resources or processes that store, transmit or process information will have no more privileges than necessary to be able to fulfil their function;
8. All relevant regulatory and legislative information security requirements will be met;
9. All breaches of information security, actual or suspected, must be reported to the Monitoring Officer;
10. All OPCC managers are responsible for the implementation of Information Security Policies within their areas;

11. Disregard for the OPCC's security policies may be regarded as misconduct to which the OPCC's dismissal and disciplinary procedure shall apply and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal;
12. All staff are responsible for upholding this policy, under the guidance and with assistance of the Monitoring Officer; and
13. The OPCC will provide appropriate security awareness training to all staff and provide specific security training where required, thereby developing and supporting a security and risk aware culture throughout the OPCC.

Information Responsibilities for Staff

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

1. Know what information you are responsible for;
2. Make sure you achieve high standards of accuracy and quality when creating and recording any information;
3. Keep the information up-to-date;
4. Classify and protect information according to its sensitivity, value, and importance;
5. Understand how information should be handled, who should receive or have access to it;
6. Make sure the information is secured, both physically and electronically;
7. Keep information for no longer than necessary – use agreed retention and disposal schedules applicable to your information;
8. Respect people's rights to privacy and confidentiality, and to access to their own personal information;
9. Respect people's right to access information that the OPCC creates, owns or holds and assist them in accessing it;
10. Make the best use of information to deliver and improve services;
11. Report any security incidents, potential or actual losses of information or equipment to your line manager and the Monitoring Officer;
12. Understand and adhere to the OPCC's information governance policies and procedures;
13. Seek advice and guidance whenever you need it from your line manager or the Monitoring Officer;
14. 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
15. 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.