Office of Police and Crime Commissioner – Devon & Cornwall
Policy Cover Sheet

Policy Name:	Data Protection and Sharing
Version Number:	V1.0
Date:	15 July 2014
Policy Author:	Eleanor Tanner, Office Manager
Policy Authorised by:	Andrew White, Chief Executive
Policy Sign off Date:	25 September 2014
Policy signed off by:	Andrew White, Chief Executive
EIA status	

Office of the Police and Crime Commissioner – Devon & Cornwall Data Protection and Sharing Policy

Version dated:14 July 2014

1.0 Policy Statement [FOIA Open]

1.1 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.

1.2 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.

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

1.4 It fully endorses and will adhere to the Data Protection Principles summarised below:-

Personal data must be:

1. fairly and lawfully processed;
2. processed for limited and lawful purposes;
3. adequate, relevant and not excessive;
4. accurate and where necessary kept up-to-date;
5. kept for no longer than is necessary;

6. processed in accordance with the rights of the data subject;
7. kept secure;
8. transferred only to countries with adequate security.

2.0 Introduction [FOIA Open]

2.1 The Data Protection Act 1998 ('the Act') governs how organisations must process information from which a living individual can be identified (i.e. personal data) and sensitive personal data about living individuals. Its aim is to protect individuals from harm through the inappropriate or irresponsible use of data and to demonstrate respect for individuals by:

- Processing information fairly
- Being transparent about why information is needed and how it will be processed
- Where possible giving an individual a choice whether to provide the information in the first place
- Not asking for irrelevant or excessive information
- Not keeping information for longer than is necessary.

2.2 It also gives individuals the rights to have access to personal data held about them on computer or in a structured manual file (i.e. on paper), and to be informed for what purposes the data is processed and the recipients, or classes of recipients, to whom the data is or may be disclosed.

2.3 The Act creates a number of roles namely:

a. Information Commissioner - appointed by the Crown to supervise the legislation contained in the Data Protection Act 1998.

b. Data Controller - A person who determines the purposes for which and the manner in which any personal data are processed. The data controller for the Office of the Police and Crime Commissioner, is the Police and Crime Commissioner.

c. Data Subject - an individual who is the subject of personal data.

2.4 The Act also establishes a Data Protection Tribunal, which provides machinery for appeals by data users against decisions made by the Information Commissioner.

3.0 Scope [FOI Open]

3.1 This policy applies to all staff within the Office of the Police and Crime Commissioner, and to agency, associated and affiliated workers and relates to all personal data and sensitive personal data collected and processed by the Office of the Police and Crime Commissioner in the conduct of its business, in electronic format in any medium, and within structured paper filing systems.

3.2 The Police and Crime Commissioner is registered with the Information Commissioner's Office (ICO) for collecting and using personal data.

3.3 Details of the full registration with the Information Commissioner can be found on the ICO website http://ico.org.uk/esdwebpages/search by quoting registration number Z3447559.

4.0 Policy Objectives [FOIA Open]

4.1 The objectives of this policy are that:

- Systems are in place for the processing of personal data that are compliant with the Act.
- There is a culture of best practice and staff are supported to comply with the Act.
- All staff understand their responsibilities when processing personal data and that methods of handling are clearly understood.
- Individuals wishing to access their personal data are aware of how to do this.
- Subject Access requests are dealt with in accordance with the Act.
- Individuals are assured that their personal data is processed in accordance with the Data Protection Principles, is kept secure at all times and is safe from unauthorised access, alteration, use or loss.
- Data sharing or transferring is compliant with the Act.
- Any new data holding or processing systems are risk assessed to ensure compliance with this policy.

5.0 Data collection and processing [FOIA Open]

5.1 The Office of the Police and Crime Commissioner will comply with the 8 Data Protection Principles by adhering to the following values when processing personal data:

- The conditions in Schedules 2 and 3 of the Act (Appendices 2 and 3) regarding the collection and use of personal data will be fully complied with.
- Those who receive and process information will ensure, so far as is possible, that it is accurate, valid and up-to-date.
- Retention of personal data will be in accordance with the Office of the Police and Crime Comissioner's Information Retention and Disposal Policy and Schedules.
- Individuals whose personal information is held on OPCC contact databases will be provided with the option to 'opt out' of receiving event invitations and future communications.
- The ICO will be informed of any intended new purposes for processing personal data. No new purpose for processing data will take place until the ICO has been notified of the relevant new purpose and the data subjects have been informed, or in the case of sensitive personal data, their consent has been obtained.

6.0 Security [FOIA Open]

6.1 In accordance with the organisation's Information Security Policy, the Office of the Police and Crime Commissioner will:

- Comply with all applicable legislation, regulations and any other adopted requirements as a minimum.
- Comply with government procedures in respect of protectively marked information. The appropriate protective markings will be used to protect and secure any document containing personal and sensitive personal information.
- Implement a risk based approach to information security when assessing and understanding the risks and will use physical, personnel, technical and procedural means to achieve appropriate security measures.
- Continually monitor its level of security.
- Take into account developments in technology and the costs of implementation in order to achieve a level of security appropriate to the nature of the information and the harm which may result from a security breach.
- Assess the integrity and identity of staff employed by the Police and Crime Commissioner and monitor compliance with their obligations with respect to data protection and information security.
- Provide appropriate data protection and information security education and awareness training to enable all staff to handle and protect personal data held by the Office of the Police and Crime Commissioner and to carry out their roles in a secure manner.

6.2 In addition,

- Any unauthorised use of corporate email, including sending of personal or sensitive personal data to unauthorised persons, or use that brings the organisation into disrepute will be regarded as a breach of this policy.
- All actual, near miss or suspected data breaches will be reported to the Chief Executive for investigation. Lessons learnt during the investigation of breaches will be relayed to those processing information to enable necessary improvements to be made.
- An information asset register will be maintained identifying personal data held, where it is held, how it is processed and who has access to it.
- There will be a member of staff who has specific responsibility for data protection.

7.0 Data sharing [FOIA Open]

7.1 In accordance with the Data Protection Act, personal data will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7.2 Personal data collected and processed by the Office of the Police and Crime Commissioner as described in the Register held by the ICO (registration number Z3447559) may, on occasion, need to be shared. Decisions to share data will be in accordance with the 9 ‘purposes’ recorded in the register and will have full regard to the Information Commissioner’s Code of Practice on Data Sharing.

7.3 A Memorandum of Understanding for the processing of data is in place between the Office of the Police and Crime Commissioner and the Devon and Cornwall Police Force.

8.0 Access [FOIA Open]

8.1 Access by staff to personal data will only be permitted where it is required as part of their functional remit.

8.2 Individuals have a right of access to personal data held about them. There is no obligation to supply information unless the request is made in writing, the prescribed fee is paid and sufficient information is given to trace the data. A data subject's personal information will not be disclosed to them until their identity has been verified. Subject access requests will be acknowledged within 3 working days, and will be processed promptly (subject to exemptions) within 40 calendar days.

8.3 Third party requests for personal data will be dealt with in accordance with the Freedom of Information Act and by reference to the Data Protection Act. Personal data will not be released to a third party when responding to a Freedom of Information request or a Subject Access request unless release is in compliance with either of these Acts.

8.4 The Office of the Police and Crime Commissioner's website will include a contact address and guidance for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how the OPCC is processing their data, or about the OPCCs handling of their request for information.

9.0 Non-disclosure exemption [FOIA Open]

9.1 Principle 2 of the Data Protection Act states that 'personal data shall be processed for limited and lawful purposes'.

9.2 The Act contains certain exemptions which permit the disclosure of personal data when necessary for:

a. National security: disclosure for the purpose of safeguarding national security;
b. Prevention or detection of crime, the apprehension or prosecution of offenders, only where the application of those provisions in relation to the disclosure would be likely to cause serious prejudice;
c. The assessment of collection of any tax or duty, only where the application of those provisions in relation to the disclosure would be likely to cause serious prejudice;
d. Disclosure required by enactment, by any law or by order of a court;
e. Disclosure for the purpose of obtaining legal advice or in connection with any legal proceedings;
f. In the following cases:
    (1) Disclosure to the data subject or to a person acting on their behalf;
    (2) Disclosure at the request or with the consent of the data subject;
    (3) Disclosure by the chief officer to their servant or agent;
    (4) Reasonable belief that (1), (2) or (3) apply.
g. Disclosure urgently required to protect the vital interests of any person or persons.

9.3 The decision to use a non-disclosure exemption will be made on a case by case basis.

9.4 If a request is made for information using a non- disclosure exemption and there are no reasonable grounds for using the exemption, then the request is unlawful and a criminal offence may be committed (section 55 (1) (3) of the Data Protection Act 1998).

10.0 Audit / Assessment Compliance [FOIA Open]

10.1 This policy has been drafted and audited to comply with the principles of the Human Rights Act. Equality and diversity issues have also been considered to ensure compliance with Equality legislation and policies. In addition Data Protection, Freedom of Information, and Health and Safety issues have been considered. Adherence to this policy will therefore ensure compliance with all relevant legislation and internal policies.

11.0 Review [FOIA Open]

11.1 The review of the contents of this policy is the responsibility of the Chief Executive. Review of the policy will be undertaken annually.

12.0 Useful Links [FOIA open]

- Information Security Policy
- Information Retention and Disposal Policy
- Memorandum of Understanding for the processing of data between the OPCC and the Devon and Cornwall Police

13.0 Appendices [FOIA Open]

Appendix 1 - Definitions

Data	information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).
Personal data	Data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and 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. .
Sensitive personal data	Personal data consisting of information as to - (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. .
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 – (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.
Data subject	An individual who is the subject of personal data.
Data controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Subject Access Request	A right most often used by individuals who want to see a copy of the information an organisation holds about them, and includes the right to be told whether any personal data is being processed; given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; given a copy of the information comprising the data; and given details of the source of the data (where this is available
Recipient	In relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.
Third party	In relation to personal data, means any person other than – (a) the data subject, (b) the data controller, or

	(c) any data processor or other person authorised to process data for the data controller or processor.

Appendix 2 - Schedule 2 of the Data Protection Act 1998

The first principle of the Act requires personal data to be processed fairly and lawfully, and not to be processed unless one of the conditions in Schedule 2 (below) is met.

1	The data subject has given his / her consent to the processing.
2	Processing is necessary for: a) The performance of a contract to which the data subject is a party, or b) The taking of steps at the request of the data subject with a view to entering into a contract
3	Processing is necessary for compliance with any legal obligations to which the data controller is subject, other than an obligation imposed by contract.
4	Processing is necessary in order to protect the vital interests of the data subject.
5	Processing is necessary for the: a) Administration of justice b) The exercise of any functions of either House of Parliament c) Exercise of any functions conferred on a person under any enactment d) Exercise of any functions of the Crown or a government department e) Exercise of any other function of a public nature carried out in the public interest by any person
6	a) Processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom data may be disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. b) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Appendix 3 - Schedule 3 of the Data Protection Act 1998

Under the first Data Protection Principle, sensitive personal data must not be processed unless one of the following legitimate conditions from Schedule 3 of the Act (below) is met.

1 The data subject has given his explicit consent to the processing of the personal data.

2(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

3 The processing is necessary—

(a) in order to protect the vital interests of the data subject or another person,in a case where—
(i)consent cannot be given by or on behalf of the data subject, or
(ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing—

(a) is carried out in the course of its legitimate activities by any body or association which—
(i)is not established or conducted for profit, and
(ii)exists for political, philosophical, religious or trade-union purposes,
(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6 The processing—
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7(1) The processing is necessary—
(a) for the administration of justice,
(aa) for the exercise of any functions of either House of Parliament,
(b) for the exercise of any functions conferred on any person by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

7A(1) The processing—
(a) is either—
(i)the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or
(ii)any other processing by that person or another person of sensitive personal data so disclosed; and
(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.
(2) In this paragraph “an anti-fraud organisation” means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8(1) The processing is necessary for medical purposes and is undertaken by—(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9(1) The processing—
(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.