Data Protection Policy

Document Author	
Richard Andrews	Acting Head of Governance and Policy - OPCC

Document Owner	
James Payne	Chief Executive – OPCC

Document location
\\ousvr\users\Office of the Police & Crime Commissioner\OPCC Policy and Procedures

Version history			
Ver No.	Version date	Requester of change	Summary of change(s)
v1.1	Aug-18	n/a – first draft	n/a – first draft
V1.2	Sept-18	Richard Andrews	Formatting update

Distribution list	
Name	Department / Organisation
Michael Lane	Police and Crime Commissioner – Hampshire and Isle of Wight
James Payne	Chief Executive - OPCC
Richard Andrews	Acting Head of Governance and Policy - OPCC
Laura Cadd	Head of Communications & Engagement - OPCC
Dave Green	Estate Director - OPCC
Alan Hagger	Head of Strategic Commissioning & Partnerships - OPCC
Anja Kimberley	Head of Performance & Information - OPCC
Andrew Lowe	Chief Finance Officer - OPCC
Enzo Riglia	Assistant Police & Crime Commissioner, Criminal Justice - OPCC
Nadia Siouty-Burke	Programme Office Lead - OPCC
OPCC Internet pages	

Table of contents

1 Introduction

1.1 The Police and Crime Commissioner (PCC) is a registered Data Controller (registration no.Z3653467). The PCC is committed to conducting its business in accordance with the data protection laws. During the course of our activities we will collect, store and process personal data about our service users, employees, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 PCC employees are obliged to comply with this policy when processing personal data.

1.3 The types of personal data that the PCC may be required to handle include information about service users, employees and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (together referred to as the Data Protection Legislation).

1.4 This policy, along with the PCC's **General Privacy Notice** https://www.hampshire-pcc.gov.uk/privacy-policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources and in accordance with the Data Protection Legislation.

1.5 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

1.6 The Data Protection Officer is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer at: opcc.dataprotection@hampshire.pnn.police.uk

1.7 The Data Protection Officer will be responsible for completing the annual registration to the ICO and advising them of any changes to the register.

1.8 For the purposes of clarity, the term PCC is used to encompass the person elected as the PCC and any staff authorised to work for or on their behalf or under their direction and control (*i.e*. the Office of the Police and Crime Commissioner or "OPCC").

2 Definition of Data Protection terms

2.1 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

2.2 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, a unique reference number, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

2.3 **Data Controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with GDPR. The PCC is the data controller of all personal data it collects or uses in its day to day business and in providing services.

2.4 **Data Processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it includes suppliers, providers and contractors which handle personal data on the PCC's behalf.

2.5 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, viewing, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

2.6 **Special Category Data** (also known as "sensitive personal data") includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. The definition also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation. Special Category Data can only be processed under strict conditions. Personal Data relating to criminal convictions and offences is subject to additional requirements and should be handled in a similar way to Special Category Data.

2.7 **Third Party** - Any individual/organisation other than the data subject, the data controller (the PCC's) or its agents.

2.8 **Data Protection Impact Assessment** is a process to help identify and minimise the data protection risks of a project. A DPIA should be carried out for processing that is likely to result in a high risk to individuals. The DPIA must: describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks.

3 Responsibilities under the General Data Protection Regulation (GDPR)

3.1 The PCC is a Data Controller under GDPR; it is also a Processor of information for other organisations.

3.2 The Chief Executive has delegated authority to carry out all functions and responsibilities of the Data Controller, although liability remains with the PCC as a corporation sole.

3.3 The Data Protection Officer is responsible for ensuring compliance with GDPR and with this policy and may assign officers to support this process.

3.4 Compliance with Data Protection legislation is the responsibility of everybody who processes personal information.

3.5 The PCC, through its staff, is responsible for ensuring that any personal data supplied is accurate and up-to-date.

4 Data Protection Principles

4.1 Anyone processing personal data must comply with the six principles relating to processing of personal data in the GDPR. These provide that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency'). For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in GDPR. These include, among other things, processing is necessary:
  - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the PCC;
  - for the performance of a contract to which the data subject is party;
  - for compliance with a legal duty;
  - the data subject has given consent for the data to be processed for a specific purpose(s).

  When special category data (sensitive personal data) is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. We will only process personal data for specific purposes. We will notify those

purposes to the data subject when we first collect the personal data or as soon as possible thereafter.

- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation'). Personal data, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If personal data is given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

- **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'). Personal Data, which is kept for a long time, must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that personal data held by the PCC is accurate and up-to-date. Individuals should notify the PCC of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the PCC to ensure that any notification regarding change of circumstances is noted and acted upon.

- **Kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required. On occasion, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR.

- **Processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5 Notifying Data Subjects

5.1 If we collect personal data directly from data subjects, we will inform them through our Privacy Notices about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The legal basis for processing.

(c) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(d) The length of time that we will retain the data.

(e) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

5.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information within the required timescales.

5.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and the contact details of our Data Protection Officer.

6 Data Security

6.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

6.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

6.3 Personal data will only be transferred to a data processor who has provided sufficient guarantees to implement appropriate technical and organisational measures that will comply with the Data Protection legislation and ensure that data subjects rights are protected and that these requirements are governed by a contract or other legally binding agreement.

6.4 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the personal data should access it;

(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed;

(c) Availability means that authorised users should be able to access the personal data if they need it for authorised purposes.

6.5 Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas will be reported;

(b) Secure lockable desks and cupboards. Desks and cupboards will be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.);

(c) Methods of disposal. Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required;

(d) Equipment. PCC employees will ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended;

(e) IT Security. IT provision is provided for the PCC by the Hampshire Constabulary/Thames Valley Police Joint ICT Department. A condition of use is compliance with the security policies of Hampshire Constabulary. A copy of the IT Security Management Policy is attached as **Appendix A**.

6.6 Training for staff includes:

(a) Mandatory training for all staff on Data Protection, with refresher training;

(b) Training for specialist Data Protection staff, including those who handle Subject Access Requests;

(c) Training for new starters as part of the corporate induction process.

6.7 Governance and assurance procedures include:

(a) Internal and external audits of the PCC's Information Management processes and procedures;

(b) For new data collection processes the PCC will ensure that a Data Protection Impact Assessment is conducted in conjunction with the Data Protection Officer for all new and/or revised systems or processes.

7 Disclosure and sharing of Personal Information

7.1 We will only disclose or share a data subject's personal data where we are legally permitted to do so, in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, service users or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

8 Individual's rights under GDPR

8.1 Individuals have a number of rights under GDPR including the right to:

- ask the PCC if it holds personal information about them;
- ask what it is used for;
- be given a copy of the information (subject to certain exemptions);
- be given details about the purposes for which the PCC uses the information and of other organisations or persons to whom it is disclosed;
- ask for incorrect data to be corrected;

- be given a copy of the information with any unintelligible terms explained;
- be given an explanation as to how any automated decisions taken about them have been made;
- ask that information about them is erased ("right to be forgotten");
- ask the PCC not to use personal information:
  - for direct marketing; which is likely to cause unwarranted substantial damage or distress;
  - to make decisions which significantly affect the individual, based solely on the automatic processing of the data.

8.2 These rights are not absolute, if the PCC is unable to respond to a request, it will outline the legal reasons for its decision clearly.

8.3 Further information can be found in our **General Privacy Notice** https://www.hampshire-pcc.gov.uk/privacy-policy, by contacting the Data Protection Officer or on the ICO's website**:** https://ico.org.uk

9 Dealing with Subject Access Requests

9.1 The PCC has provided application forms on its website to assist data subjects to make a request to access information we hold about them. Data subjects do not have to use our forms or use any particular wording. A subject access request is valid if it is submitted by any means, *i.e*. in a letter, an email or verbally. Employees who receive a request should pass it without delay to the Data Protection Officer.

9.2 Any individual who wishes to exercise this right should provide satisfactory proof of identity and sufficient information to enable the data to be located.

9.3 Subject to satisfactory completion of 9.2 above, the PCC should respond within one month.

9.4 There are some limited circumstances in which personal data relating to the applicant may be withheld. Examples of this include repeat access requests, confidential references, and third party information.

9.5 Further information can be found in the PCC's Subject Access Policy and Procedure.

10 Dealing with a Data Security Breach

10.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

10.2 A data security breach must be reported to the Data Protection Officer without delay to be recorded and reported as appropriate.

10.3 Further information can be found in the PCC's Data Breach Policy and Procedure.

11 Retention and disposal of data

11.1 The PCC discourages the retention of personal data for longer than they are required. Personal data must be disposed of in a way that protects the rights and privacy of data subjects (*e.g*. shredding, disposal as confidential waste, secure electronic deletion).

11.2 The PCC maintains a Retention Policy and a Retention Schedule that is specific and relevant to specific types of information and the services they relate to. These outline the appropriate periods for retention.

11.3 Where the PCC deviates from its Retention Schedule it will record the reasons why and will indicate how long the information will be retained.

11.4 Further information can be found in the PCC's Retention and Disposal Policy.

12 Use of CCTV

12.1 The PCC's use of CCTV is regulated by the Surveillance Camera Commissioner. The PCC complies with the Surveillance Camera Code of Practice and the ICO Code of Practice under the Data Protection Act 1998. It is anticipated a new Code under the GDPR and DPA 2018 will be produced in due course, supplemented by local policy and guidance.

APPENDIX A: HAMPSHIRE CONSTABULARY

IT SECURITY MANAGEMENT POLICY

28400 POLICY – IT SECURITY MANAGEMENT

Version	2.2	Last updated	30/01/2014	Review date	08/01/2018
Equality Impact Assessment			Low		
Owning department			Joint Information Management Unit (JIMU)		

1. About this Policy

1.1. The objective of this policy is to provide direction and support for IT Security in accordance with business requirements and relevant laws and regulations.

1.2. This policy outlines Hampshire Constabulary's approach to the protection of its IT infrastructure. This policy is intended to prevent major and widespread damage to Constabulary assets such as the network, user applications, files, and hardware.

1.3. The policy applies to all Hampshire Constabulary staff (permanent and temporary personnel), contractors and third parties with contractual obligations to maintain Force IT systems.

2. General Principles

2.1. Information systems represent essential core assets to the daily operation of the Constabulary. Availability, performance and security of the network including its computers and systems are key to service delivery.

2.2. New viruses represent a continual threat, requiring continual research to plan proactive measures against them.

2.3. Information systems are subject to the discovery of operating system or application vulnerabilities and the subsequent emergence of exploits of such vulnerabilities which have the potential to cause disruption or damage to those systems.

2.4. Hampshire Constabulary recognises that there may be legitimate business needs for members of the Constabulary and other third parties to be able to access information systems on the Constabulary's network from remote locations that are not linked directly to the network.

3. Statement of Policy

3.1. Asset Management

3.1.1. Responsibilities for assets

3.1.2. Objective – To achieve and maintain appropriate protection of Hampshire Constabulary assets

Inventory of assets	Control All assets shall be clearly identified and an inventory of all information security assets drawn up and maintained.
Ownership of assets	Control All information and assets associated with information processing facilities shall have nominated Information Asset 'Owners'.
Acceptable use of assets	Control Rules of acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented in the form of Security Operating Procedures (SyOPs).

3.2. Communications and Operations Management

3.2.1. Operational Procedures and Responsibilities

3.2.2. Objective – To ensure the correct and secure operation of information processing facilities

Documented operating procedures	Control Operating procedures shall be documented, maintained and made available to all users who need them.
Change management	Control Changes to information processing facilities and systems shall be controlled.
Segregation of duties	Control

	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of Hampshire Constabulary's assets.
Separation of development, test and operational facilities	Control Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.

3.2.3. Third Party Service Delivery Management

3.2.4. Objective - to implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

Service delivery	Control It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.
Monitoring and review of third party services	Control The services, reports and records provided by third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
Managing changes to third party services	Control Changes to the provision of services, including maintaining and improving exiting information security policies, procedures and controls, shall be managed, taking into account of the criticality of business systems and processes involved and re-assessment of risks.
Remote Access	Control Remote access by third parties will be uniquely identified, subjected to robust risk analysis and supported via contracts between the Constabulary and the third party. All request for remote access will be authorised by the Sy&IA Unit.

3.2.5. System Planning and Acceptance

3.2.6. Objective – to minimise the risk of systems failures

Capacity management	Control The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
System acceptance	Control Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

3.2.7. Protection Against Malicious and Mobile code

3.2.8. Objective – to protect the integrity of software and information.

Controls against malicious code	Control Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented, these will include the provisions to detect, remove and protect against viral infections. All computers connected physically or remotely to the Hampshire Constabulary network will have anti-virus software correctly installed, configured, activated, and up-dated with the latest version of virus definitions.
Controls against mobile code	Control Where the use of mobile code is authorised, the configuration shall ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code shall be prevented from executing.
Patch Management	Control Critical system updates will be deployed as soon as practicable, after an assessment of risks and ensuring patch stability. Where patching of the infrastructure us not a viable option other security measures will be sought.

3.2.9. Back-up

3.2.10. Objective – to maintain the integrity and availability of information processing facilities.

Information back-up	Control Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

3.2.11. Network Security Management

3.2.12. Objective – to ensure the protection of information in networks and the protection of the supporting infrastructure.

Network controls	Control The network will be adequately managed and controlled in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.
Security of network services	Control Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

3.2.13. Media Handling

3.2.14. Objective – to prevent unauthorised disclosure, modification, removal or destruction of assets and interruption to business activities.

Management of removable media	Control There shall be documented procedures in place for the management of removable media.
Disposal of media	Control Media shall be disposed of securely and safely when no longer required, using formal procedures.
Information handling procedures	Control Procedures for the handling and storage of information shall be established to protect this information from unauthorised disclosure or

	misuse.
Security of system documentation	Control System documentation shall be protected against unauthorised access.

3.2.15. Exchange of Information

3.2.16. Objective – To maintain the security of information and software exchanged within Hampshire Constabulary and with any external entity.

Information exchange policies and procedures	Control Formal exchange policies, procedures and controls shall be in place to protect the exchange of information through the use if all types of communication facilities.
Information Sharing agreements	Control Agreements shall be established for the exchange of information and software between Hampshire Constabulary and external parties.
Physical media in transit	Control Media containing information shall be protected against unauthorised access, misuse or corruption during transportation beyond Hampshire Constabulary's physical boundaries.
Electronic messaging	Control Information involved in electronic messaging shall be appropriately protected.
Business information systems	Control Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems

4. Implications of the Policy

4.1. The implementation of the required information security standards will incur substantial resource implications for the Hampshire Constabulary. The cost of physical and technical security controls required for new initiatives will be included in their procurement.

5. Monitoring / Evaluation

5.1. Monitoring for compliance with this policy is the responsibility of the Joint Information Management Unit. The Force Information Security Policy and associated documents are independently evaluated by the CJX / Airwave Accreditor as part of the annual process for seeking to renew the Force's Codes of Connection to those national services.

6. Review

6.1. This policy and all associated documents will be every three years or more frequently as deemed necessary.

7. Other Related Policies, Procedures and Information Sources

7.1. 06100 Policy - Information Security

7.2. AD203 - Equality Impact Assessment

7.3. Information sources:
HMG IA Standards
CESG Good Practice Guides
Security Policy Framework
ISO 27001

Origin: Joint Information Management Unit (JIMU)

APPENDIX B: SPECIAL CATEGORY AND CRIMINAL OFFENCE PERSONAL DATA APPROPRIATE POLICY DOCUMENT

1. Introduction

1.1 In accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) this document outlines where processing of special category and criminal offence personal data is needed for:

a) Performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with **employment** (Article 9 (b) GDPR)
b) Reasons of **substantial public interest** (Article 9 (g) GDPR)

1.2 This policy document should be read in conjunction with the Police and Crime Commissioner's (PCC) Data Protection Policy.

2. Definitions

2.1 **Special Category Data** (Article 9 GDPR) includes information revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data or biometric data
- Health data
- Data on a person's sex life or sexual orientation

2.2 **Criminal Offence Data:** Article 10 of the GDPR applies to personal data relating to criminal convictions and offences, or related security measures (Criminal Offence Data). The Information Commissioner's Office guidance says the concept of criminal offence data includes the type of data about criminal allegations, proceedings or convictions that would have been sensitive personal data under the 1998 Act. However, it is potentially broader than this as Article 10 specifically extends to personal data linked to related security measures.

3. The Data Protection Principles

3.1 Article 5 of the GDPR sets out six principles relating to processing of personal data. These provide that personal data must be:

- **Processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency').

- **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes.

- **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation').

- **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

- **Kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected.

- **Processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

3.2 The PCC will process data covered by this policy in accordance with the six data protection principles.

4. Processing necessary to carry out obligations under employment law

4.1 The special category personal data that it is necessary to process to carry out obligations under employment law is health data relating to employees.

4.2 The processing of health data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or data subject in connection with employment (paragraph 1 (1) (a) of Schedule 1 to DPA 2018).

4.3 The PCC requires health data on an employee to carry out its duty to make reasonable adjustments under the Equality Act 2010. The PCC will not request health data before a conditional job offer is made.

4.4 Employees will be provided with a privacy notice explaining the lawful basis for processing the data.

4.5 The data will not be used for any other purpose than the original purpose or as permitted by law.

4.6 The PCC will only collect the minimum personal data that we need for the purpose it is collected.

4.7 The PCC will ensure the data is accurate and kept up to date where necessary.

4.8 The PCC will retain and dispose health data in accordance with its Retention Schedule.

4.9 It is likely that health data on an employee will be retained during the course of employment and for six years after their employment has ended. The data will be disposed of securely.

4.10 If an applicant receives a job offer but decides not to accept, it is likely any health data will be retained for six months and then disposed of securely.

5. Processing necessary for reasons of substantial public interest

5.1 The special category and criminal offence personal data it is necessary to process for reasons of substantial public interest is:

- Health data relating to volunteers
- Criminal records relating to volunteers
- Race, ethnicity, religious beliefs, sexual orientation and health of volunteers and employees (i.e. equal opportunities data)

Health data relating to volunteers

5.2 The processing is necessary for the exercise of a function conferred on the PCC by law and for reasons of substantial public interest (paragraph 6 (1) and (2) (a) of Schedule 2 to DPA 2018).

5.3 The PCC carries out the Independent Custody Visiting (ICV) Scheme as part of its functions under sections 1 and 5 of the Police Reform and Social Responsibility Act 2011 (the 2011 Act) and section 51 of the Police Reform Act 2002. Independent custody visitors are volunteers. The PCC recruits the volunteers. The PCC needs health data on volunteers to comply with its duty to make reasonable adjustments and to protect their welfare in a custody environment.

5.4 Volunteers will be provided with a privacy notice explaining the lawful basis for processing the data.

5.5 The data will not be used for any other purpose than the original purpose or as permitted by law.

5.6 The PCC will only collect the minimum personal data that we need for the purpose it is collected.

5.7 The PCC will ensure the data is accurate and kept up to date where necessary.

5.8 The PCC will retain health data in accordance with its Retention Schedule.

5.9 It is likely that for unsuccessful applicants, data will be securely disposed of within six months of the outcome of the application.

5.10 It is likely that for volunteers health data will be retained whilst they volunteer and for six years after they stopped volunteering.

Criminal records relating to volunteers

5.11 The processing is necessary for the exercise of a function conferred on the PCC by law and for reasons of substantial public interest (paragraph 6 (1) and (2) (a) of Schedule 2 to DPA 2018).

5.12 As mentioned above the PCC carries out the ICV Scheme as part of its functions under the 2011 Act and the Police Reform Act 2002. PCC recruits volunteers to carry out the visits. The PCC needs to carry out a vetting procedure on prospective volunteers to assess their suitability.

5.13 Volunteers will be provided with a privacy notice explaining the lawful basis for processing the data.

5.14 The data will not be used for any other purpose than the original purpose or as permitted by law.

5.15 The PCC will only collect the minimum personal data that we need for the purpose it is collected.

5.16 The PCC will ensure the data is accurate and kept up to date where necessary.

5.17 The PCC will retain criminal records data in accordance with its Retention Schedule.

5.18 It is likely that for unsuccessful applicants, criminal records data will be securely disposed of within six months of the outcome of the application.

5.19 It is likely that for volunteers criminal records data will be retained whilst they volunteer and for six years after they stopped volunteering.

<u>Equal opportunities data relating to employees and volunteers</u>

5.20 The processing of race, ethnicity, religious beliefs, sexual orientation and health of volunteers and employees is necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between specified groups of people with a view to enabling such equality to be promoted or maintained (paragraph 8 (1) of Schedule 1 to DPA 2018).

5.21 The PCC carries out equal opportunities monitoring as a part of its public sector equality duty under s149 of the Equality Act 1990. The PCC carries out monitoring in respect of its employees and volunteers.

5.22 Employees and volunteers will be provided with a privacy notice explaining the lawful basis for processing the data.

5.23 The data will not be used for any other purpose than the original purpose or as permitted by law.

5.24 The PCC will only collect the minimum personal data that we need for the purpose it is collected.

5.25 The PCC will ensure the data is accurate and kept up to date where necessary.

5.26 The PCC will not carry out processing for the purposes of measures or decisions in relation to a particular individual.

5.27 The PCC will not carry out processing if it is likely to case substantial damage or substantial distress to an individual.

5.28 The PCC will not carry out processing where an individual has given written notice requiring that we do not process the data provided the notice gave us a reasonable period in which to stop the processing the data.

5.29 The PCC will retain the data and dispose of the data in accordance with the Retention Schedule. The PCC will anonymise the data and then securely destroy it as soon as possible thereafter.

6. RECORDS

6.1 Under Article 30 of the GDPR the PCC is required to keep a record of processing activities. Where processing is carried out under this policy the record of processing must include the following information:

- which condition is relied on (i.e. in Schedule 1 of the DPA 2018)
- how the processing satisfies Article 6 of the GPPR (lawfulness of processing) and
- whether the personal data is retained and erased in accordance with the Retention Schedule and if it is not the reasons for departing from the Schedule.

7. CONTACT US

7.1 If you have any queries please contact our Data Protection Officer at the Office of the Police and Crime Commissioner for Hampshire, St George's Chambers, St Georges Street, Winchester Hampshire SO23 8AJ

Telephone: 01962 871595 (Monday-Friday, 9.00am-4.00pm)

Email: opcc.dataprotection@hampshire.pnn.police.uk