Data Protection and Freedom of Information Policy

From May 2018

1. Introduction

1.1 The Office of the Police and Crime Commissioner is a Data Controller and a Data Processer under the General Data Protection Regulation May 2018 (GDRP).

1.2 The GDPR states that:

Anyone who processes personal information must comply with eight principles of Data Protection, which make sure that personal information is:

- **fairly** and **lawfully** processed;
- **secure** and **confidential**;
- processed for specific purposes which is **explicit, legitimate** and stated at the time of the data collection;
- **adequate, relevant** and **necessary**;
- kept for a specified **minimum length of time**, and kept **accurate** and **up to date**, otherwise the data should be **rectified** or **deleted**;
- processed in a **transparent** way, so that people understand the **purpose** and **extent** of the processing and who the Data Controller is. The information may be **clear, accessible** and **easy to understand**.

- line with your **rights** and that you are aware of the **risks, rules** and **safeguards**;

1.3 All Data Controllers have a responsibility to make sure they protect personal data and keep it secure. We will take action to make sure we don't process unlawfully and to stop data being accidentally lost or destroyed.

1.4 The Office of the Police and Crime Commissioner for Avon and Somerset (OPCC) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. This policy sets out the expected requirements for staff of the OPCC in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to an individual who has contacted the OPCC, such as you (i.e. the Data Subject). This policy is to assist the PCC and staff in processing personal data in line with the General Data Protection Regulation (GDPR) legislation by promoting good practice in all its operations. It is essential that all information is collected, used, stored and disposed of in ways that protect its confidentiality, integrity and availability. The data is in various forms such as personal, financial and operational information and some of it may be sensitive (referred to as 'Special Categories of Data'). We are committed to providing effective management of data and the safeguarding of personal information.

2. Scope

2.1 This policy deals with personal data that is relevant to the day to day running of the OPCC. It covers information relating to those who contact the OPCC, whose personal data may be logged and held. This policy applies to all processing of personal data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

3 Definitions

Child under 13 year old

Consent Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Contact Any past or current person who contacts the OPCC

Data Controller A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor A natural or legal person, public authority, agency or other body which processes personal data on behalf of a Data Controller.

Data Protection The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Subject The identified or identifiable natural person (see definition below) to which the data refers.

Employee An individual who works part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes volunteers, temporary employees and independent contractors.

Identifiable Natural Person Anyone who can be identified from the data or from the data and other information which is in possession of, or is likely to come into the possession of, the data controller. The information may be in either electronic or manual format.

Personal data Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Information which relates to a living individual who can be identified from the data or from the data and other information which is possession of, or is likely to come into the possession of, the data controller. The information may be in either electronic or manual format.

Personal data Breach A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Process, Processed, Processing Any operation performed on personal data. This may include collecting, recording, using or destroying data.

Profiling Any form of automated processing of personal data where personal data is used to carry out analysis. The OPCC does not currently profile any data.

Third Party An external organisation with which the OPCC conducts business.

4 Governance

4.1 Avon and Somerset Constabulary will appoint a Data Protection Officer (DPO) who will be shared with the OPCC. In the interim the OPCC Chief Executive will be the DPO.

4.2 The Data Controller is the PCC.

4.3 The DPO (once appointed) will report to the OPCC Chief Executive.

5 Data Protection by Design

5.1 Our current processes have been reviewed to ensure that all Data Protection requirements have been identified and addressed.

5.2 To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

5.3 For new data collection processes, the lead staff member in the OPCC must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in conjunction with the DPO, for all new and/or revised systems or processes for which the OPCC. Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the DPO to assess the impact of any new technology uses on the security of personal data.

6 Compliance Review

6.1 To ensure best practice is used across the organisation and to monitor and update processes on a regular basis, the lead staff member, in conjunction with the Chief Executive, will carry out an annual Data Protection compliance review. This will include assessment of:

- Data collection and processing
- Processing of Right of Access requests
- The Privacy Notice
- Policy reviews
- Staff training and awareness
- Security protocols
- Data transfers
- Data retention policy compliance

Any deficiencies will be addressed within the OPCC.

7 GDPR Principles

The OPCC will comply with the principles for GDPR as follows:

- **Lawfulness, Fairness and Transparency**

  Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, the OPCC must tell the Data Subject what processing will occur (transparency), the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

- **Purpose Limitation**

  Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the OPCC must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

- **Data Minimisation**

  Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the OPCC must not store any personal data beyond what is strictly required.

- **Accuracy**

  Personal data shall be accurate and kept up to date. This means the OPCC must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

- **Storage Limitation**

  Personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. This means the OPCC must, wherever possible, store personal data in a way that limits or prevents identification of the Data Subject.

- **Integrity & Confidentiality**

  Personal data shall be 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. The OPCC must

use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

- **Accountability**

  The Data Controller shall be responsible for, and be able to demonstrate, compliance. This means the OPCC must demonstrate that the Data Protection Principles (outlined above) are met for all personal data for which it is responsible.

- **Data Protection by Design and Default**

  See section 5 above.

8 How and why we collect and process data

The Avon and Somerset OPCC's lawful basis for processing information comes under the following categories:

- Legitimate interest – responding to queries, running of events, providing media statements and press releases.
- Consent – passing information over to Avon and Somerset Police where this is appropriate.
- Contract – issuing grants and commissioning services.
- Legal obligation – dealing with complaints against Avon and Somerset Constabulary's Chief Constable, against the PCC or members of OPCC staff, Human Resources (HR) data and applications.

We collect data from a Data Subject if they have contacted us to request information or action to be taken and we are the appropriate body to carry out that request. We also collect data when we have contacted a person with regard to organising an event or when a person has applied for a role. We collect statutory information when processing complaint information.

The OPCC uses the personal data of its contacts for the following broad purposes:

- To enable us to provide information or action for the benefit of residents in the Avon and Somerset Policing area or others with a legitimate interest, including media;
- To manage and maintain our records and accounts;
- To communicate with residents in the Avon and Somerset Constabulary area, our communities or partners about events and service;
- To process HR information;
- To deal with complaints against the Chief Constable, PCC and OPCC staff;
- To raise a concern for a person's welfare or wellbeing.

Data is collected via email, telephone, in person, via letter or social media. It is collected on a database for contacts, for information or a complaint. Digital marketing data will be collected on a recognised event software product. For HR data this is collected manually and may be kept electronically.

Personal data should be collected only from the Data Subject unless one of the following applies:

- The nature of the purpose necessitates collection of the personal data from other persons or bodies;
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person;

If personal data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following applies:

- The Data Subject has received the required information by other means;
- The information must remain confidential due to a professional secrecy obligation;
- A national law expressly provides for the collection, processing or transfer of the personal data;

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal data;
- At the time of first communication if used for communication with the Data Subject;
- At the time of disclosure if disclosed to another recipient.

9 Consent

9.1 The OPCC will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, the OPCC is committed to seeking such consent.

9.2 Where the Data Subject wishes the OPCC to pass their information on to Avon and Somerset Police in order to receive an appropriate response with OPCC involvement, this information will be passed to Avon and Somerset Police and the Data Subject informed. Personal data will be kept by the OPCC to keep a record of the query and response received.

9.3 Where the Data Subject has contacted the OPCC and not wanted Avon and Somerset Police involvement, their consent will be sought before passing personal details to Avon andAvon and Somerset Somerset Police. There are two exceptions to this:

- Complaints: Where the OPCC receives a compliant about a member of Avon and Somerset Police Officers or staff, or about Avon and Somerset Police processes we are required to pass this on to Avon and Somerset Constabulary.
- Concern for welfare or safety: Where the OPCC received contact where there are concerns for the Data Subject, or another individual's safety and well-being, we will pass this on to Avon and Somerset Police.

9.4 Where a Data Subject contacts the OPCC and the request relates to information held by another organisation we will ask the Data Subject to contact that organisation directly. We will still record personal data in this case.

9.5 Children: The OPCC does not specifically market itself towards or encourage contact directly with children (defined as those who are under 13). Children are unable to Consent to the processing of personal data. If personal data is collect with regard to a child, consent must be sought from the person who holds parental responsibility over the child. For legal purposes, that is a complaint or a concern for welfare of a child, consent does not need to be sought.

10 Privacy Notice and Data Access

10.1 The OPCC will, when required by applicable law, by contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the processing of their personal data.

10.2 When the Data Subject requests disclosure of their personal information held by the OPCC, disclosure will be made unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or consent.

10.3 The OPCC will make available the OPCC Privacy Notice on our website.

10.4 The OPCC will also publish a Right of Access form, to allow for Data Subjects to request access to their data, request deletion or request amendment.

11 Data Quality and Data Retention

11.1 The OPCC will ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject. The measures adopted by the OPCC to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification;
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period. This is listed in the published Record Retention Schedule;
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required;
- Restriction, rather than deletion of personal data, when:
    - A law prohibits erasure; or
    - Erasure would impair legitimate interests of the Data Subject.
    - The Data Subject disputes that their Personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

11.3 Digital marketing. As a general rule the OPCC will not send promotional or direct marketing material to a Data Subject through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent.

11.4 Data Retention. To ensure fair processing, personal data will not be retained by the OPCC for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which the OPCC need to retain personal data is set out in the Retention Schedule, available on the OPCC website.

12 Information security

12.1 The PCC 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 PCC's premises and computer equipment;
- Ensuring the protection of electronic systems;
- Restricting staff access to those who require personal data for their work;
- Comply with government procedures in respect of protectively marked information.

12.2 For further information please refer to Avon and Somerset Constabulary's Information Security Manual - designed to achieve appropriate protection for information whether held on pape or electronically, whether corporate or operational, and including evidence.
https://pocketbooksite.com/Interact/Pages/Content/Document.aspx?id=1377&SearchId=

12.3 The purpose of the policy is to protect the business of both the OPCC and Avon and Somerset Police 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.

12.4 Refer also to the OPCC Privacy Notice. This document explains how the Avon and Somerset Police & Crime Commissioner (the PCC) obtains, holds, uses and discloses information about people - their personal information1 -, the steps taken to ensure that it is protected, and also describes the rights individuals have in regard to their personal information handled by the PCC.

16.5 All actual, near miss or suspected data breaches should be reported to the Data Processing Officer. Please refer to the OPCC Breach policy. Lessons learnt will be relayed to those processing information to enable necessary improvements to be made.

16.6 The Joint Operating Policy Information Management details the processing of data between the OPCC and Avon & Somerset Police.

13 Data Subject Rights

13.1 Once individuals have provided personal data to the OPCC, individuals then have the following rights:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object.
- Rights in relation to automated decision making and profiling. (Note: The OPCC do not use information collected in this way.)

13.2 If an individual makes a request relating to their personal data processed by the OPCC, the OPCC will consider each request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

13.3 Data Subjects are entitled to obtain, based upon a request made in writing to the OPCC and upon successful verification of their identity, the following information about their own personal data:

- The purposes of the collection, processing, use and storage of their personal data;
- The source(s) of the personal data, if it was not obtained from the Data Subject;
- The categories of personal data stored for the Data Subject;
- The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients;
- The envisaged period of storage for the personal data or the rationale for determining the storage period;
- The use of any automated decision-making, including Profiling;
- The right as the Data Subject to:
    - object to processing of their personal data;
    - lodge a complaint with the Data Protection Authority;
    - request rectification or erasure of their personal data;
    - request restriction of Processing of their personal data.

13.4 All requests received for access to or rectification of personal data must be sent to the OPCC to log each request as it is received. A response to each request will be provided without dealy and no later than a month after receipt of the request.

13.5 Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

13.6 Data Subjects shall have the right to require the OPCC to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

13.7 If the OPCC cannot respond fully to the request within one month then the OPCC will provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request;
- Any information located to date;
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision;
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature);

13.8 It should be noted that situations may arise where providing the information requested by a Data Subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that third person's rights.

13.9 Detailed guidance for dealing with Access Rights and requests from Data Subjects can be found in the OPCC Privacy Notice.

14 Vetting Procedure

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

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

14.2 All PCC employees allowed access to police information or assets will follow the instructions contained in Avon and Somerset Constabulary's Vetting Procedure. Failure to conform to those instructions may result in a vetting refusal, disciplinary, or criminal action.

14.3 It will be the responsibility of the PCC's employee - and the PCC's Office & HR Manager - to report to the Constabulary's Vetting Officer all matters which may affect the staff member's vetting status at the earliest opportunity.

14.4 For further information regarding the Police and Crime Commissioner's vetting procedure please refer to Procedural Guidance – Vetting Policy.

15 Freedom of Information Act 2000

15.1 The Office of the Police and Crime Commissioner (OPCC) is fully committed to complying with the Freedom of Information Act 2000 (FOIA) and its principles of openness and accountability of public authorities.

15.2 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 and 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 covers written requests for information made to the Police and 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 and Crime Commissioner and, if so, the information should be supplied to them, unless one of the exemptions available under the Act applies.

15.3 All PCC employees have a responsibility:

- To recognise a request for information that falls within the FOIA. Requests must be in writing and provide the person's full name and contact details but do not have to mention the Act. Such requests should be passed to the

Public Contacts and Standards Officer in the first instance. A request must not be refused unless:

- the information is already provided as part of the publication scheme. In this case, the applicant must be directed to the scheme.
- there is an exemption under the FOIA under which the information does not have to be provided
- the request is vexatious (a request that has been made several times)
- the cost involved in meeting the request is disproportionate.

- Employees should ensure that all requests for information are dealt with within 20 working days.
- The Chief Executive must be informed when information is to be published or otherwise made available that has not previously been so. This is to ensure that the Police & Crime Commissioner's publication scheme is kept up to date.
- A harm test and a public interest test must be applied if a qualified exemption is being considered.

Appeals Procedure

15.4 If, for any reason, an applicant is not satisfied with the FOI response they receive, they have the right to appeal against their decision through the OPCC Appeals Procedure. If not satisfied with the outcome of the appeal they then have the right to appeal directly to the Information Commissioner.

OPCC Publication Scheme

15.5 The Publication Scheme specifies what information the OPCC will make routinely available to the public as a matter of course. The OPCCs Publication Scheme is available on the website. The Office & HR Manager is responsible for updating the scheme.

Policy Statement Information	
Policy Owner (Job Title)	Chief Executive
Date to be Reviewed	May 2019
Date Last Reviewed Completed	May 2018
Effective Commencement Date	May 2018