Office of the Police and Crime Commissioner for Surrey

Surrey OPCC
Data Protection Policy
From July 2020

Reviewed July 2020
Next Review: July 2021

Table of Contents

Introduction

The Office of the Police and Crime Commissioner is a Data Controller and a Data Processer under the Data Protection Act 2018 (DPA) & General Data Protection Regulations May 2018 (GDPR).

The GDPR states that:

Anyone who processes personal information must comply with principles of the Data Protection Act:

1. Personal data shall be processed lawfully, fairly and in a transparent manner
2. Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date
5. Personal date shall be kept in a form which permits identification of data subjects for no longer than necessary
6. Personal data shall be processed in a manner that ensures appropriate security of the personal data

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 informally unlawfully and to stop data being accidentally lost or destroyed.

The Office of the Police and Crime Commissioner for Surrey (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 OPCC contact (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. We are committed to providing effective management of data and the safeguarding of personal information.

Scope

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.

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 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.

Governance

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, the OPCC has appointed a Data Protection Officer (DPO) who is shared with Surrey Police, and Data Protection Lead Officer (DPLO) who is the OPCC Chief Executive.

The Data Controller is the PCC. The PCC has delegated day to day responsibility for Data Control to the OPCC Chief Executive.

The DPO reports to the OPCC Chief Executive and to the Head of Service Quality and the Chief Information Officer within Surrey Police.

Data Protection by Design

Our current processes have been reviewed to ensure that all Data Protection requirements have been identified and addressed and if required, we will carry out a Data Impact Assessment.

Compliance Review

To ensure best practice is used across the organisation and to monitor and update processes on a regular basis, the DPLO, supported by the OPCC Office Manager, will carry out an annual Data Protection compliance review. This will include assessment of:

- Data collection and processing
- Processing of with Rights of Access requests
- Privacy Notices
- Policy reviews
- Staff training and awareness
- Security protocols
- Data transfers
- Data retention policy compliance

Any deficiencies will be addressed by the DPLO in with the OPCC team.

GDPR Principles

The OPCC will comply with the 6 principles for GDPR as follows:

Principle 1: 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 (in Privacy Notice) 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).

Principle 2: 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 purpose. This means the OPCC must specify exactly what personal data is collected and for what it will be used.

Principle 3: 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.

Principle 4: 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.

Principle 5: 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.

Principle 6: 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 six Data Protection Principles (outlined above) are met for all personal data for which it is responsible.

How and why we collect and process data

The Surrey OPCC 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 Surrey Police where this is appropriate
- Contract – issuing grants and commissioning services
- Legal obligation – dealing with complaints against the Chief Constable or members of OPCC staff, dealing with Surrey Police complaint review requests. 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 the public of Surrey or others with a legitimate interest, including media
- To manage and maintain our records and accounts
- To communicate with Surrey residents, communities or partners about events and service
- To process HR information
- To process Surrey Equity Loans (a previously set-up home-buying scheme for police officers which is no longer available but still has some members of the scheme)
- To deal with complaints against the Chief Constable and members of OPCC Staff
  To deal with Surrey Police complaint review requests
- To raise a concern for a person's welfare or wellbeing

Data is collected via e-mail, telephone, in person, via letter or social media. It is collected on a database for contact for information or a complaint. For events management data may be collected on a recognised event software product. For HR data this is collected manually and may be kept electronically. The recruitment advertisement and application process is handled by Surrey Police's Recruitment Team on behalf of the PCC. Some HR processes, payroll functions etc. are also processed by the Surrey Police HR and Payroll Department on behalf of the PCC. The PCC has an Information Sharing agreement with the Chief Constable of Surrey Police for this purpose.

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.

Consent

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.

Where a Data Subject contacts the OPCC and the request relates to information held by Surrey Police we will ask the Data Subject to contact Surrey Police directly. We will not record personal data in this case.

Where the Data Subject wishes the OPCC to pass their information onto Surrey Police in order to receive and appropriate response with OPCC involvement, this information will be passed to Surrey Police and the Data Subject informed.

Personal data will be kept by the OPCC to keep a record of the query and response received.

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

- Complaints – where the OPCC receives a compliant about a member of Surrey Police staff or Surrey Police processes we are required to pass this onto Surrey Police
- Concern for welfare or safety – where the OPCC received contact where there are concerns for the Data Subject, or another individuals, safety and well-being, we will pass this onto Surrey Police.

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 not record personal data in this case.

Privacy Notice and Data Access

The OPCC will, when required by applicable law, 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.

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.

The OPCC will make available the OPCC Privacy Notice on their website.

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

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 for Information Society Services. 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.

Data Quality

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 and inform other parties if this is shared data.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period
- 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, insofar as:
    - A law prohibits erasure.
    - 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.

Digital Marketing

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

Where personal data processing is collected for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes.

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 OPCC need to retain personal data is set out in the Retention Schedule, available on the OPCC website.

How we protect data

The OPCC adopts physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

A summary of the Personal data related security measures is as follows:

- protecting records held on computer with permissions managed to ensure access is restricted only to those who are entitled to access files;
- restricting access to OPCC files, which are kept on the Surrey Police server, from wider Surrey Police access;
- keeping paper files in a secure location with access limited to authorised staff;
- transmitting personal data electronically to secure e-mail addresses;
- data is never stored on pen drives or other removable media unless encrypted and then only for the purpose of secure delivery;

- using secure delivery methods such as “guaranteed delivery” if sending personal data through the post;
- regularly backing up electronic files through Surrey Police IT systems;
- ensuring that premises are properly protected with burglar and fire alarms.

Data Rights of Access Requests

Individuals 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. (The OPCC do not use information collected in this way.)

If an individual makes a request relating to their personal data processed by the OPCC, the DPLO, in conjunction with the DPO, will consider each such 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. 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 right of 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

All requests received for access to or rectification of Personal data must be directed to the DPLO Office who will log each request as it is received. A response to each request will be provided within one calendar month of the receipt of the written request from the Data Subject.

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

Data Subjects shall have the right to require the OPCC to correct or supplement erroneous, misleading, outdated, or incomplete Personal data if they can provide proof that it is incorrect.

If the OPCC cannot respond fully to the request within one calendar month, the DPLO shall nevertheless 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);
- The name and contact information of the Diocesan individual who the Data Subject should contact for follow up.

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 person's rights and there may be further exemptions that apply.

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

Complaints Handling

Data Subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the DPLO. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The DPLO will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the data subject and the Data Compliance Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation via the Information Commissioner's Office (ICO).

Breach Reporting

Any individual who suspects that a Personal data Breach has occurred due to the theft or exposure of personal data must immediately follow the OPCC's Data Breach Procedure set out for staff in the Data Protection Procedures.

A brief summary of actions required include:

- Immediately alert the line manager;
- Document the breach details;
- Inform the DPO and the ICO where appropriate
- Inform the Data Subject
- Make every effort to contain the breach to ensure no further data is lost, corrupted or accessed.

Drafted: July 2020

Approved by: Alison Bolton, OPCC Chief Executive