Data Protection Policy

The Legal Framework

The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Data Subjects rights

Under the Data Protection Act 2018, data subjects have the right to find out what information the government and other organisations store about them. These include the right to:

- be informed about how their data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of their data
- data portability (allowing the data subject to get and reuse their data for different services)
- object to how their data is processed in certain circumstances

Data Subjects also have rights when an organisation is using their personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict behaviour or interests

Definition of Data Protection terms

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 of 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 Controllers are people, or organisations, who determine the purposes for, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with GDPR.

Data Protection Officers are responsible for overseeing an organisation's data protection policy and its implementation to ensure compliance with GDPR requirements.

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 an organisation's behalf.

Data Subjects for the purpose of this policy include all living individuals about whom an organisation holds 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.

Employee is 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 is 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 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.

Personal Data Breach is 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.

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.

Data Protection is the process of safeguarding personal data from unauthorised or unlawful disclosure, access and changes to be made on behalf of a Data Controller.

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.

Third Party - Any individual/organisation with which organisations conduct business.

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.

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.
The 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 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.

The Office of the Police and Crime Commissioner is a Data Controller and a Data Processor under the Data Protection Act 1998 (DPA) and General Data Protection Regulations May 2018 (GDPR).

Governance

The PCC's Chief Executive is a Data Controller under GDPR. 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 data informally or unlawfully and to stop data being accidentally lost or destroyed.

The Head of Governance is the Data Protection Officer (DPO) and is responsible for ensuring compliance with GDPR and with this policy and has assigned the Governance and Compliance Manager with supporting this process.

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

All staff have a responsibility to ensure that their activities comply with the data protection principles. Staff should not disclose personal data outside of OPCC procedures, or use personal data held on others for their own purposes.

The OPCC is responsible for ensuring that any personal data supplied is accurate and up-to-date.

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

To ensure best practice is used across the OPCC and to monitor and update processes on a regular basis, the Governance and Compliance 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 Chief Executive and Solicitor.

Data Protection Principles

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

- **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. See section How and why we collect and process data on the next page.

  When special category data (sensitive personal data) is being processed, additional conditions must be met. When processing personal data we will ensure that those requirements are met.

- **Collected for specific, 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 all personal data is accurate, having regard to the purposes for which it is processed, erased or rectified without delay (accuracy). Personal Data, which is kept for a long time, will be reviewed and updated as necessary. No personal data will be kept unless it is reasonable to assume it is accurate. Data subjects are asked to notify us of any changes in circumstances to enable their personal records to be updated accordingly. It is our responsibility to ensure that any notification regarding change of circumstances is noted and acted upon.

- **Kept in form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data is processed. We will not keep personal data longer than is necessary for the purpose or purposes for which it was 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. Further information can be found in the **Retention and Disposal Policy**.

- **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). Further information can be found in the **Information Security policy**.

How and why we collect and process data

Our 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 South Yorkshire Police where this is appropriate
- Contract – issuing grants and commissioning services
- Legal obligation – dealing with complaints against the Chief Constable or members of the OPCC staff, 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 South Yorkshire or others with a legitimate interest, including media
- To manage and maintain our records and accounts
- To communicate with South Yorkshire residents, communities or partners about events and service
- To process HR information
- To deal with complaints against the Chief Constable and members of 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 contact for information or a complaint.

Events management data may be collected on a recognised event software product. HR data is collected manually and may be kept electronically. The recruitment advertisement and application process is handled by South Yorkshire Police's Recruitment Team, on behalf of the PCC. Some HR processes, payroll functions etc. are also processed by South Yorkshire Police. The PCC has a Memorandum of Understanding for Provision of Non-Operational Business Support with the Chief Constable of South Yorkshire 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 directly from the Data Subject, the OPCC will inform them through its Privacy Notices about:

- The purpose or purposes intended to process that personal data.
- The legal basis for processing.
- The types of third parties, if any, the Data Subject's personal data will be disclosed to.
- The length of time the personal data will be retained.

- The means, if any, with the Data Subject can limit the use or disclosure of their personal data.

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 disclosure to another recipient.

Consent

We 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**,** we will always seek such consent.

Where a Data Subject contacts us and their information is held by South Yorkshire Police, we will ask the Data Subject to contact South Yorkshire Police directly. We will not record personal data in this case.

Where the Data Subject wishes us to pass their information onto South Yorkshire Police in order for us to provide an appropriate response, this information will be passed to South Yorkshire Police and the Data Subject informed.

Personal data will be kept to record queries and responses received.

Where the Data Subject has contacted us and not wanted South Yorkshire Police involvement, their consent must sought before passing personal details to South Yorkshire Police. There are two exceptions to this:

- Complaints – where we receive a compliant about a member of South

Yorkshire Police staff, or South Yorkshire Police processes, we are required to pass this onto South Yorkshire Police
- Concerns for welfare and safety – where we have concerns for the Data Subject, or another individual's, safety and wellbeing, we will pass this onto South Yorkshire Police.

Where a Data Subject requests 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 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.

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

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

Children

If aged under 13 parental consent is required. Once the individual reaches the age of 13 parental consent is no longer valid and consent from the child must be obtained in order to continue to lawfully process their personal data.

Data Quality

We will ensure that the personal data collected and processed 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

- 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 we 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

We discourage the retention of personal data for longer than it is 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).

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

Any deviation from the Retention Schedule requires approval of the DPO and a record of the reasons why and an indication of how long the information is to be retained will be made.

Further information can be found in the **Retention and Disposal Policy**.

How we protect data

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

The OPCC 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.
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.

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

- Confidentiality means that only people who are authorised to use the personal data should access it;
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed;
- Availability means that authorised users should be able to access the personal data if they need it for authorised purposes.

Security procedures include:

- Entry controls. Any stranger seen in entry-controlled areas will be reported;
- 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);
- Methods of disposal. Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required;
- Equipment. Employees will ensure that individual monitors do not show confidential information to passers-by and that they lock their PC when it is left unattended;
- IT Security. IT provision is provided by the South Yorkshire Pension Authority. A condition of use is compliance with the security policies of South Yorkshire Police.

Further information can be found in the **Information Security Policy**.

Disclosure and Sharing of Personal Information

The OPCC will only disclose or share a Data Subject's personal data where there is a legal basis to do so, in order to comply with any legal obligations, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect the rights, property, or safety of employees, service users or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

Data Rights of Access Requests

Once individuals have provided personal data to the OPCC, individuals have a number of rights under GDPR including the right to:

- ask if we 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 we use 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 us 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.

These rights are not absolute. Where we unable to respond to a request, we will outline clearly the legal reasons for this.

Further information can be found in our General Privacy Notice, by contacting the Governance and Compliance Manager or on the ICO's website: https://ico.org.uk/

Dealing with Subject Access Requests

A subject access request (SAR) is valid if it is submitted by any means, i.e. in a letter, an email or verbally.

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

Subject to satisfactory completion of the above, we should respond within one calendar month. For example, a SAR received on 3 September should be responded to by 3 October.

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.

Further information can be found in the **Subject Access Policy**.

Dealing with a Data Security Breach

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.

A data security breach must be reported to the Governance and Compliance Manager without delay to be recorded and reported as appropriate.

Further information can be found in the PCC's **Data Breach Policy**.

Implementation Date	01/12/2019
Author	S Parkin
Review Date	30/11/2021