Office of the Police and Crime Commissioner for Cleveland

OPCC Data Protection Policy

Policy Owner	
[redacted]	[redacted]

VERSION CONTROL

Version	Date	Author	Reason for Change

Table of contents

1 Introduction

2 Definition of Data Protection terms

3 Responsibilities under GDPR

4 Data protection principles

5 Informing data subjects

6 Information security

7 Disclosure and sharing personal information

8 Subject rights under GDPR

9 Subject access requests

10 How to deal with a personal data breach

11 Retention and disposal

1 Introduction

1.1 The Police and Crime Commissioner (PCC) is a registered Data Controller (registration no. ZA000699). The Office of the Police and Crime Commissioner (OPCC) conduct a range of activities in pursuit of implementing the PCC's Police and Crime Plan. The OPCC is committed to upholding data protection legislation and encouraging good practice in information management and security.

1.2 Some of the business the OPCC conducts involves collecting, storing and processing the personal data of service users, employees, suppliers and other third parties. The security and protection of this information is of the upmost importance to us and we have developed this policy to ensure people can have trust in the integrity of our policies and procedures.

1.3 The types of personal data that the OPCC may be required to handle include information about the general public, commissioned services and suppliers, employees and others that we communicate with.

1.4 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 (herein after described throughout this policy as 'the Act').

Aim of this policy

1.5 The main aim of this policy is to ensure that personal information owned, stored and processed by the OPCC is used appropriately in compliance with the requirements of the Act and that all officers and staff are clear about what is regarded as acceptable and what is improper use.

1.6 The policy is underpinned by procedures that set out details about how those employees and any other authorised person with access to OPCC systems may use personal data lawfully.

Principles and scope of this policy

1.7 The OPCC is committed to ensuring that all officers, staff and contractors collect, store and process information in a manner compatible with data protection principles set out in the GDPR and the Act.

1.8 The Act regulates the use of information from which a living individual can be identified. It applies to the processing of personal data in most formats including electronic, paper and other media.

1.9 One key objective is to protect individuals from the use of inaccurate personal information, or the misuse of accurate personal information.

1.10 More specific associated objectives include:

- Ensuring all OPCC staff with access understand their responsibilities regarding the use of personal information;
- Eradicate all unlawful use of personal information;
- Safeguard personal information held by the OPCC;
- Maintain the reputation of the OPCC by having strict compliance with GDPR and the Act.

1.11 The Data Protection Officer (DPO) is responsible for ensuring compliance with 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.

1.12 The DPO is responsible for completing the annual registration to the Information Commissioner's Office and advising them of any changes.

Failure the comply with the policy

1.13 All OPCC employees who have access to personal information must be aware of, and are required to comply with, all relevant policy and associated procedures.

1.14 This policy applies to persons at all levels of the organisation including all OPCC employees, temporary staff, agency staff, consultants, contractors and volunteers.

1.15 The OPCC will take disciplinary and/or criminal action against any person in a role mentioned above whom wilfully accesses and/or misuses personal information held by the OPCC.

1.16 Any use of personal information that does not have a clear statutory or business purpose is likely to constitute a misuse. Using information is described as "processing" in the Act. See Part 1 3(4) of the Act that describes the ways in which data is defined as having been processed (used).

1.17 Part 6 Section 166 of the Act identifies the following criminal offence:

A person must not knowingly or recklessly, without the consent obtain or disclose personal data or the information contained in the personal data or procure the disclosure to another person of the information contained in personal data.

2 Definition of Data Protection terms

2.1 **Data subject** – The data subject is the identified or identifiable living individual to whom personal data relates.

2.2 **Personal data** - Any information relating to a person (a 'data subject') who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

2.3 **Data controller(s)** - A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Only controllers need to pay the data protection fee.

2.4 **Data processor(s)** - A person, public authority, agency or other body which processes personal data on behalf of the controller. The distinction between this role and the controller lies in the decision-making; each can process data, but the processor does not make decisions about the data or how it is processed.

2.5 **Processing** - In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

2.6 **Special category data** - The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection:

- Personal data revealing racial or ethnic origin;
- Personal data revealing political opinions;
- Personal data revealing religious or philosophical beliefs;
- Personal data revealing trade union membership;
- Genetic data;
- Biometric data (where used for identification purposes);
- Data concerning health;
- Data concerning a person's sex life;
- Data concerning a person's sexual orientation.

The recitals to the GDPR explain that these types of personal data merit specific protection. This is because use of this data could create significant risks to the individual's fundamental rights and freedoms.

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 (DPIA** - A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. A must be completed for processing that is likely to result in a high risk to individuals. It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

3 Responsibilities under GDPR

3.1 Under the GDPR, the PCC is the Data Controller.

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

3.3 The Data Protection Officer is responsible for ensuring compliance with GDPR and the Act. They are responsible for compliance 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 OPCC, through its employees, is responsible for ensuring personal data is accurate and up-to-date.

4 Data protection principles

4.1 The GDPR sets out six key data protection principles. These principles are the cornerstone of good data protection practice and should be adhered to by all people who process personal data:

- **Lawfulness, fairness and transparency**

  Data must be: *"Processed lawfully, fairly and in a transparent manner in relation to the data subject"*

  - For processing of personal data to be **lawful,** it must be based on a "legal basis" to do so, as set out in the GDPR. If no lawful basis applies then processing will be unlawful and in breach of this principle. We will identify a legal basis for all of our processing.
  - We will achieve **fairness** by ensuring personal data is only handled in ways that people would reasonably expect and not used in ways that have unjustified adverse effects on them.
  - **Transparent** processing is about being clear, open and honest with people from the start about our organisation, and how and why we use their personal data. We inform them of this through our privacy notices, which are displayed on our website.

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.

- **Purpose limitation**

Data must be: *"Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"*

- We will ensure that we are **clear and open** about our reasons for obtaining personal data, and that processing of the data is in line with the **reasonable expectations** of the individuals concerned.
- We will help individuals understand how their data will be used, so they can make decisions about whether they are happy to share their details, and assert their rights over data where appropriate.
- We understand that this is fundamental to building **public trust** in how personal data is being used.

- **Data minimisation**

Data shall be: *"Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*

- We will identify the **minimum amount** of personal data needed to fulfil the specified purpose for processing and not storing any additional data which is surplus to requirements.
- Information collected will be **adequate** to fulfil the stated purpose, **relevant** to this purpose and **limited** to what is necessary.

- **Accuracy**

Data shall be: "*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"*

- We will take reasonable steps to ensure the **accuracy** of any personal data and will ensure the source and status of personal data is clear.
- We will consider whether it is necessary to **periodically update** the information.
- Should someone **challenge** the accuracy of data held, careful consideration will be given to their claim.
- If it is discovered that personal data is incorrect or misleading, we will take reasonable steps to **correct or erase it** as soon as possible.

- **Storage limitation**

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 are processed"*

- We will carefully **consider and justify** how long we hold personal data, and document this in the OPCC Retention and Disposal Policy.
- We will **not keep personal data any longer than is necessary**, and will review information we hold and erase it when we no longer need it.

- Individuals have the **right to erasure** and we will carefully consider any challenges to our retention of data.

- **Security**

  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, using appropriate technical or organisational measures"*

  - We understand the **risks** presented by our data processing and use this to assess the **level of security** we put in place, whether a physical or technical measure.
  - We adhere to Cleveland Police's Information Security Policy and take steps to make sure it is implemented in the OPCC.
  - The measures we put in place ensure the 'confidentiality, integrity and availability' of our systems and services and the personal data we process within them.

- **Accountability**

This principle is about how we take responsibility for complying with GDPR, at the highest level of management and throughout our organisation.

- We will keep evidence of the steps we have taken to comply with GDPR.
- We will put in place technical and organisational measures, including:
  - Adopting and implementing data protection policies;
  - Taking a 'data protection by design and default' approach – putting data protection at the centre of developing new processing operations
  - Documenting our processing activities and implementing necessary security measures;
  - Recording, and where necessary, reporting personal data breaches;
  - Carrying out data protection impact assessments for new uses for personal data which may result in high risk to subjects
  - Appointing a data protection officer.
- We will review these measures at appropriate intervals.

5 Informing data subjects

5.1 When we collect personal data from subjects, we will inform them through our privacy notices about:

- The type of personal data that we collect;
- Where we collect data from;
- The purpose(s) for which we intend to process that personal data;
- The legal basis for processing;

- Whether we intend to share any of their personal data with a third party organisation;
- How we keep their information safe;
- And how long we plan to retain their information for.

5.2 We will let the data subject know that we are the data controller under GDPR and provide contact details for our Data Protection Officer.

6 Information Security

6.1 We will take appropriate security measures against the unauthorised access or loss of personal data.

6.2 We utilise technology and procedure to protect personal data from the moment we collect it until its 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 As defined in the GDPR, our security measures will ensure the 'confidentiality, integrity and availability' of our systems and services:

- **Confidentiality** – Personal data will only be accessed, altered, disclosed or deleted by those with authorisation to do so;
- **Integrity** – The data we hold is accurate and complete in relation to our reasons for processing it;
- **Availability** – Our data remains accessible and useable to authorised users.

6.5 Our security protocols include:

a) **Access controls** – Any unauthorised person within the Central Police Headquarters and specifically the OPCC offices / working environment, will be challenged.

b) **IT Security** – IT provision and support is provided for the OPCC by the Cleveland Police ICT Department. A condition of use is compliance with the security policies of Cleveland Police. A copy of the IT Security Management Policy is attached as **Appendix A.**

c) **Storage** – Archived paper records are stored in a secure off-site storage facility.

d) **Lockable cupboards** – Confidential and organisationally sensitive information can be locked in the tambour units number 13,21 and 20. The Monitoring Officer and Data Protection Officer currently had keys for these units**.**

e) **Equipment** - OPCC staff are responsible for ensuring that laptop screens are locked when unattended and for ensuring their laptop is stored in a secure place

when not in use. Privacy protectors for laptop screens and other privacy equipment can be provided for those working remotely in public locations.

f) **Day books** – All OPCC staff should be using a personal issue notepad or 'day book', which should be handed back to the organisation once filled.

g) **Disposal** – Physical records and documents should be shredded or placed in confidential waste as soon as they are no longer needed. Digital storage devices (e.g USB drive) should be destroyed.

6.6 Training for staff is essential to ensuring good information management and adherence to this policy. Training includes:

a) Mandatory e-learning training for all OPCC staff via NCALT.

b) Specialist training for staff who work in compliance and disclosure, including staff who handle Freedom of Information requests.

c) Training for new starters on this policy with the DPO as part of our programme of induction.

6.7 To ensure this policy is being delivered across the organisation, the following governance and assurances process are in place:

a) Internal and external audits of the OPCC's Information Management processes and procedures.

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

7 Disclosure and sharing 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;
- In order to enforce or apply any contract with the data subject or other agreements;
- To protect our rights, property, or safety of our employees, service users or others.

8 Subject rights under GDPR

8.1 The GDPR provides the following rights for individuals:

- **The right to be informed** – We must provide individuals with our purpose(s) for processing their personal data, our retention periods for that personal data, and who it will be shared with.

- **The right of access** - Individuals have the right to access their personal data and we must provide what information we hold on them if they submit a 'subject access request'.
- **The right to rectification** - Individuals have the right to ask us to rectify inaccurate personal data, or to complete any incomplete records.
- **The right to erasure –** Also known as the 'right to be forgotten'. We must delete or erase any information we hold on an individual should they make a request.
- **The right to restrict processing** - Individuals have the right to request the restriction or suppression of their personal data**.** This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the personal data, but not use it.
- **The right to data portability** - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- **The right to object** - The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- **Rights in relation to automated decision making and profiling** - We can only carry out this type of decision-making where the decision is necessary for the entry into or performance of a contract, authorised by Union or Member state law applicable to the controller or based on the individual's explicit consent.

8.2 These rights are not absolute, if the OPCC 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.cleveland.pcc.police.uk/Information/Privacy-Notice.aspx, or by contacting the Data Protection Officer or on the ICO's website**:** https://ico.org.uk

9 Subject access requests

9.1 The OPCC has created a dedicated email address to assist data subjects to make a request for the information we hold about them. Subjects do not need to make a request via this specific email address. A subject access request is valid if it is submitted by any means, i.e. in a letter, an email or verbally or via social media. Employees who receive a request should pass it without delay to the Data Protection Officer / Deputy Data Protection Officer.

9.2 Sufficient information is required for us to fulfil a subject access request. If we require any further information from a requester, or proof of their identity, we will seek this without delay.

9.3 The OPCC should respond to any subject access request within one month.

9.4 There are some circumstances in which we may refuse to comply with a subject access request, namely if an exemption applies, if the request is 'manifestly unfounded', if the request is 'excessive' or it relates to third party data. If we refused to comply with a

request we must provide a full explanation to the requester and inform them of their right to appeal.

10 How to deal with a personal data 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 personal data breach must be reported to the Data Protection Officer (or in their absence, the Monitoring Officer) without delay and reported, if appropriate.

11 Retention and Disposal

11.1 We will not store any personal data longer than is necessary and will actively discourage this to our staff. 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 OPCC maintains a Retention and Disposal Policy and a Retention Schedule which sets out retention periods for specific types of information we hold and the areas of business they relate to.

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

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

CONTACT US

If you have any queries, please contact our Data Protection Officer at our postal correspondence address c/o St Marks House, St Marks Court, Thornaby, Stockton-On-Tees, TS17 6QW

Telephone: 01642 301208

Email: rachelle.kipling@cleveland.police.uk