# Policy: Data Protection

## Equality Statement

The Office of the Police and Crime Commissioner (OPCC) is committed to the principles of equality and diversity. No member of the public, member of staff, contractor, volunteer or job applicant shall be discriminated against on the grounds of age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; or sexual orientation.

We are committed to ensuring the privacy and security of your personal data. For more information, please visit our Privacy Notice

## Introduction

This Policy covers our obligations under the Data Protection Act 2018. The Policy applies to the Office of the Police and Crime Commissioner, the Violence Reduction Partnership, and those contracted to work on our behalf, and is to be followed at all times. Its aim is to protect the rights of individuals and applies to all personal and sensitive information that is used, stored, and transmitted either electronically or via paper-based methods.

**Contents**



## Data Protection

The Data Protection Act 2018 (DPA 2018) together with UK GDPR provide the legislative framework for data protection, and this policy sets out how the Commissioner will meet the responsibilities under this framework. Data protection legislation applies to living individuals and gives those individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully. It regulates the manner in which such information can be collected, used, and stored, and so is of prime importance in the context of information sharing.

The Commissioner has appointed the Head of Business Services as the Data Protection Officer (DPO) (Decision reference number 013/2018)

The Office of the Police and Crime Commissioner is registered with the Information Commissioner's Office as a data controller. The registration number is ZA002898.

## Subject Access Requests

Under Article 15 of UK GDPR, an individual has 'The Right to Access' personal information which is being held about them. This information is to be provided free of charge and individuals have the right to obtain:

- the purposes of the processing;
- the categories of Personal Data concerned;
- the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the Data Subject or to object to such processing;
- the right to lodge a complaint with a Supervisory Authority;
- where the Personal Data are not collected from the Data Subject, any available information as to their source;

Although the information will be provided free of charge, where there is an excessive request for data, or repetitive requests a 'reasonable fee' can be charged.

Any fee charged must be based on the administrative cost of providing the information and information must be provided without delay and at the latest within one month of receipt.

We are able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

It is important that we verify the identity of the person making the request, using 'reasonable means'. If the request is made electronically, we will provide the information in a commonly used electronic format (e.g. CSV, or PDF).

1. The Commissioner will respond properly to any request for personal data. Individuals can make a subject access request to find out what information is held about them and are encouraged to use the form provided for this purpose. Individuals should note that the Commissioner will need to satisfy himself of the identity of the individual. On arrival, the request will be assessed, and a copy of the privacy notice will be made available to enable the individual to understand how their data is used. Once identity has been verified, the information will be provided within a month from the working day following the request and sooner where possible. If it is going to take longer, the individual will be notified.

2. There will be no charge for this service unless the request is manifestly unfounded, excessive or a duplicated request, in which case a reasonable fee to cover the cost of processing may be charged, in advance of the records being released. The Commissioner may exercise his right to refuse to comply with a request, and if so will state:
   - the reasons for not taking action;
   - their right to make a complaint to the ICO or another supervisory authority; and
   - their ability to seek to enforce this right through a judicial remedy.

## Data Breaches

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. When a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms.

2. Serious data breaches will be reported to the ICO. If a member of staff, contractor or volunteer loses, mislays or has any information stolen from them, they must notify the D P O immediately. If it is out of hours the staff member can contact the Out of Hours emergency media enquiries telephone in the first instance – (telephone number on the website), who will contact the Data Protection Officer.

3. The DPO will assess the severity of the breach and make a decision on whether to notify the ICO. It may be that the individuals to whom the information relates will also need to be notified. Even if the ICO is not notified every breach will be logged on the Breach Log. We will follow West Midlands Police processes so that IT equipment can be made secure.

**Data Protection Impact Assessment (DPIA)**

A DPIA is a process to analyse our processing and help to identify and minimise the data protection risks of a project. The DPIA should be undertaken at the beginning of any new work which involves processing data and may result in high risk to data protection. The DPO will need to approve the DPIA once it is finished.

A DPIA is needed if a project or new way of working involves any of the following:

- Any processing which is large scale, or which involves profiling or monitoring
- Processing which decides on access to services or opportunities
- Processing which involves sensitive data or vulnerable people
- New technologies
- Using systematic and extensive profiling with significant effects;
- Processing special category or criminal offence data on a large scale;
- Systematically monitoring publicly accessible places on a large scale.
- Use profiling or special category data to decide on access to services;
- Profile individuals on a large scale;
- Process biometric or genetic data;
- Matching data or combining datasets from different sources;
- Collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- Tracking individuals' location or behaviour;
- Profiling children or targeting marketing or online services at them; or
- Processing data that might endanger the individual's physical health or safety in the event of a security breach.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

A template is readily available to all staff in order to undertake a DPIA. The first step is an initial screening questionnaire, which is sent to the DPO. The DPO will then advise on whether or not a DPIA is required.

**Information Sharing Agreements (ISAs)**

ISAs are used in circumstances when we regularly share personal data with other organisations.

In some circumstances, it can also be useful to have an agreement in place even when personal data is not being shared. For example, it might be helpful to have an ISA to enable a shared understanding and framework if we are regularly sharing sensitive information between ourselves

and other organisations, even if this doesn't include personal data.

The role of an ISA is to:

- help all the parties be clear about their roles;
- set out the purpose of the data sharing;
- cover what happens to the data at each stage; and
- sets standards.

An ISA will include the details of the parties to the agreement, and in particular who are the data controllers.

The ISA should explain:

- purpose, specific aims and benefits of the data sharing
- names of all the organisations involved, including contact details
- what data is going to be shared
- what is the lawful basis for sharing the data
- will special category data, sensitive data or criminal offence data be shared?
- procedure for compliance with individual rights
- how the information might be disclosable under the Freedom of Information Act
- What information governance is in place

**Information Security**

The OPCC is committed to aligning ourselves with the standards set out in ISO 27001. We will do this by adhering to and falling under the umbrella of the Information Security service provided by West Midlands Police, and we will abide by their Information Security Policy.

The OPCC's approach to information security is to balance the business requirements of the organisation with the potential harm and risk of an information security incident and the cost and logistics of implementing security controls. The requirements of this Policy must be incorporated into operational and contractual arrangements. All breaches of information security, whether actual or suspected, must be reported to the Data Protection Officer. Information Security awareness, education and training will be made available to all employees, delivery partners and third-party contractors of the OPCC. The Data Protection Officer has overall responsibility for the satisfactory implementation and maintenance of the general security requirements contained in this policy.

The Information Asset Owner (IAO) is the senior individual responsible for the relevant business area and is responsible for the information process or area of work for which the information system was provided.

The IAO needs to understand what information is held, what is added and what is removed, how information is moved and who has access to it and why. As a result, the IAO will be able to understand and address risks to the information and ensure that information is fully used within the law for the public good and approved purpose of the OPCC. The IAO's must also maintain regular communication with the Data Protection Officer on all matters concerning the security of their information assets/systems.

In all circumstances, however, the IAO remains ultimately responsible for the security of the information and should be able to determine that any delegated responsibility has been discharged

correctly and as directed by the ISO.

All staff and employees of the organisation, contractors and third parties who have access to OPCC information are required to adhere to this Information Security Policy and its supporting processes and procedures.

Failure to comply with this policy (and its supporting processes and procedures) MUST be escalated to relevant risk coordinator, failure to do so may lead to disciplinary action.

**Version Control**

| Version No. | Date | Author | Post | Reason for issue | Date agreed by PCC | Review Schedule | Comments |
|---|---|---|---|---|---|---|---|
| 1.0 | June 2025 | Andrea Gabbitas | Head of Business Services | General Update | | Bi-annual | This Policy has been separated from Information Governance / Information and Records Management Policy |
| | | | | | | | |