



Confidentiality and Data Protection Policy

Relevant Definitions:

- **Personal Data:**
Personal data refers to any information that relates to an identified or identifiable individual. This can include details such as name, contact information, identification numbers, or any other information that can directly or indirectly identify a person.
- **Special Categories of Personal Data:**
Special categories of personal data are types of personal data that are considered more sensitive and require higher levels of protection. These include data related to racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, health information, and data concerning a person's sex life or sexual orientation.
- **Data Subject:**
A data subject is an individual whose personal data is being collected, stored, or processed. Essentially, it refers to the person to whom the data relates.
- **Data Controller:**
A data controller is the entity (individual or organisation) that determines the purposes and means of processing personal data. The data controller is responsible for ensuring that personal data is handled in compliance with data protection laws and regulations.

Introduction

QPCO recognises that, in the context of our work, we come into contact with people from diverse backgrounds and deal with potentially sensitive individual and community issues. Consequently, it is essential for maintaining trust and developing relationships that information is treated appropriately. This policy outlines how we will record, use, and store information, how, with whom, and under what conditions it will be shared, and how individuals can access the information.

For employees, it is a condition of employment that a breach of this confidentiality policy will be dealt with as a serious matter. Serious breaches may result in dismissal. The responsibility to adhere to this policy persists even after a person has ceased to be an employee or volunteer with QPCO.

What Are Our Responsibilities?

As a data controller, we are responsible for processing the personal data that you provide. We are required to comply with data protection laws, including the General Data Protection

Regulation (2018) and any national implementing laws or successor legislation (“Data Protection Legislation”).

We are committed to the following principles:

- Processed in a lawful, fair, and transparent way
 - Collected and processed for specified, explicit, and legitimate purposes, with a view to minimising data collection and storage
 - Accurate and processed in a manner that ensures integrity and confidentiality
 - Collected and processed in a manner that allows for accountability
-

What Kind of Information Do We Hold?

We hold the following data:

- **Organisational Information** – This is publicly available information about organisations, as well as some confidential information (such as office/employee contact numbers, which are for partner agencies and not for public use).
- **Personal Information – Public** – This includes information about individuals such as names, addresses, phone numbers, and email addresses for the purposes of advertising our work and events, etc.
- **Personal Information – Personnel** – This includes information about employees (both employed and voluntary) as necessary for maintaining relevant records (including DBS checks, as our community work involves employees engaging with children, young people, and vulnerable adults).

(Any trustee, employee, or volunteer has the right to see what information is held on file about them by sending a request to the Director.)

QPCO will only collect information for “specified, explicit, and legitimate purposes” [GDPR, Article 5, clause 1(b)].

What Is Personal Data?

Your personal data includes all the information we hold that identifies you and/or is about you. We may hold ‘special categories’ of data, as our Intervention Officers may hold information about a person’s health. We will collect only the data necessary for the purpose of advocacy and will keep it secure.

Information obtained about people through unofficial channels (e.g., gossip or hearsay) should not enter QPCO’s information system, except where non-disclosure may lead to either a legal risk or a risk to anyone’s health or safety.

We may process sensitive personal data related to race/ethnicity for the purposes of reporting to funders. We will do this only if you have explicitly consented.

What Is Processing?

Everything we do with your personal data counts as processing, including collecting, storing, amending, transferring, and deleting it. We are, therefore, required to comply with the Data Protection Legislation to ensure that your information is properly protected and used appropriately.

On What Grounds Do We Process Your Personal Data?

We may rely on different grounds to lawfully process your personal data, depending on the nature of our relationship with you. The lawful processing of your personal data will fall into these categories:

- **Consent:** The individual has given clear consent for us to process their personal data for a specific purpose.
 - **Contract:** The processing is necessary for a contract, or because we have been asked to take specific steps before entering into a contract. This includes employment contracts and contracts with suppliers.
 - **Legal Obligation:** The processing is necessary for us to comply with the law, including safeguarding laws.
 - **Vital Interests:** The processing is necessary to protect someone's life.
 - **Legitimate Interests:** The processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests.
-

Why Do We Process Your Personal Data?

We will only use your data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose.

These purposes may include:

- Making a general enquiry with us, in which case we may need your data to respond.
- Making an enquiry of our Intervention Officers, in which case we respond to you. This may include special category data, such as disability/health information, in order to advocate on your behalf.

- If you wish to attend an event, we may need personal details to fulfil your request.
- If you are providing goods or services to us.
- If you have taken part in a consultation or survey managed or commissioned by us.
- If you have applied for a volunteer role, we may need to process data.
- If you have approached us regarding a potential employment opportunity, we may need to process information provided in your CV and/or covering letter.

QPCO will only hold information for specific purposes and will inform individuals of those purposes. It will also inform them if those purposes change.

QPCO will ensure that anyone with whom it works (e.g., employees, applicants, volunteers, and personnel in partner agencies) is aware of the reasons for collecting and using any personal data.

Who Will Receive Your Personal Data?

We sometimes receive data from other organisations in the form of referrals, and we may also share personal data with partner organisations.

There may be situations where QPCO works in partnership with other organisations on projects that require data sharing. One example is the work of our Intervention Officers. QPCO will clarify which organisation is to be the Data Controller and will ensure that the Data Controller deals correctly with any data QPCO has collected.

How Do We Ensure That Your Data Is Secure?

QPCO has procedures for ensuring the security of all personal data, which will be handled “in a manner ensuring appropriate security of the personal data, including protection against unlawful processing or accidental loss, destruction or damage” [GDPR, Article 5, Clause 1(f)].

Paper records containing confidential personal data are stored and disposed of in a secure manner. Employee and personnel records (including DBS disclosure information) are held in a locked filing cabinet with regulated access. Disposal will be by shredding, pulping, or burning, and we will not allow any personal data to be kept in an insecure receptacle while awaiting disposal.

Electronic records are held on password-protected laptops, which are kept safely in a locked filing cabinet, in person with the relevant employee or volunteer, or securely in the home or

car (when being transported) of the relevant employee or volunteer. Where possible, external hard drives shall be password-protected and/or encrypted.

Emails containing personal data should be retained only for as long as necessary to fulfil the purposes for which they were collected.

How Long Will We Store Your Data?

We will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it. This can include satisfying any legal, accounting, or regulatory reporting. In determining the retention period, we consider the amount, nature, and sensitivity of the personal data and any risks associated with retaining the data.

Information will be “kept in a form which permits identification of data subjects for no longer than necessary” [GDPR, Article 5, Clause 1(e)].

The information that QPCO holds will be “accurate and, where necessary, kept up to date” [GDPR, Article 5, Clause 1(d)].

What Are Your Rights?

You benefit from a number of rights in respect of your personal data we hold about you. We have summarised your rights below, but more information is available from [ICO Guide to Data Protection](#).

1. **Right to be Informed:** You have the right to know what information is being collected and how it's being used.
2. **Right to Access:** You have the right to see your personal data. Individuals will be entitled to access the information held about them by QPCO, unless the information compromises the confidentiality of a third party.
3. **Right to Rectification:** You have the right to have inaccurate data corrected or completed.
4. **Right to Erasure:** You have the right to have your data deleted in certain circumstances. Individuals will be entitled to request the deletion of any and all records that QPCO may hold about them.
5. **Right to Restrict Processing:** You have the right to limit how your data is processed in certain circumstances.
6. **Right to Data Portability:** You have the right to obtain and reuse your data for different services.
7. **Right to Object:** You have the right to object to how your data is processed in certain circumstances.

Data Protection Principles

QPCO shall actively adopt The Six Privacy Principles of GDPR in both policy and practice, as outlined in Appendix A.

DBS Disclosure Information

DBS disclosure information is only passed to those authorised to receive it in the course of their duties. In accordance with section 124 of the Police Act (1997), it is a criminal offence to pass this information to anyone who is not entitled to receive it. The disclosure will be destroyed within 6 months or once the applicant or employee has been deemed suitable for their role. A record will be kept of the disclosure date of issue and number. Should funders require further proof, the employee will need to produce the original disclosure.

Training and Monitoring

All new employees will receive training on the data protection policy and procedures.

QPCO will carry out regular reviews of its data protection policy and procedures, especially if requirements change.

Protection of this Policy

Any employee or volunteer, and any person with whom QPCO works, has the right to complain if they feel their confidentiality has been breached in any way.

Any member of the employee/volunteer team who becomes aware of another employee/volunteer misusing confidential information or breaching this policy must report it immediately to the QPCO Secretary or to a Trustee.

Appendix A - The Six Privacy Principles of GDPR



Review Date: May 2025

Next Review Date: May 2027