People Focused Group

Data Protection Policy

UPDATED october 2022 review october 2023 [redacted]

Introduction

The People Focused Group needs to process information about employees, organisations and individuals who use our services. When we process information, we need to keep to the terms of the Data Protection Act 1998. In particular, we need to make sure that we process information in line with eight principles of data protection described in the Act. (The eight principles are listed at the bottom of page 2.)

The Data Protection Act sets limits on the way we collect, store and use information. The Act controls how:

- We file information
- How we access information
- How we pass information on to other organisations and individuals; and how and when we destroy information we are storing.
- The Act says that people have a right to access any information that we hold about them. This includes employees, PFG members and people who use our services.
- The Act says that we have to respond to requests for access to information within 40 calendar days.
- The Act says that organisations that process information need to register with the Information Commissioner's Office. There are exceptions to this rule for some not-for profit organisations. Under these exceptions, PFG does not have to register with the Information Commissioner.
- The PFG Board has overall responsibility for ensuring that PFG works in line with the Data Protection Act.
- The PFG Board, PFG staff and any others who process personal information on behalf of PFG must comply with the principles of the Act.

- **PFG's Responsibilities;**

- PFG wants to protect the right of individuals to privacy
- We will respect the privacy of individuals when processing personal information
- We will take appropriate measures to make sure that the data we hold is stored securely
- The PFG Board has overall responsibility for making sure that PFG meets the terms of the Data Protection Act
- PFG management staff have a responsibility to make sure that staff process information in line with the terms of the Act.

Staff Responsibilities

- Staff are responsible for the security of the information they process
- Staff must not pass on information to anyone who is not entitled to it
- Staff should make sure that any information they give to PFG about their employment is accurate and up to date.

Right of Access

- PFG employees, members, and people who use our services have the right to access personal information PFG holds about them, whether in electronic or paper form
- People who want to access information held about them should contact the PFG committee
- More information about individuals' right of access is available in Appendix 2

The Eight Principles of Data Protection

The Data Protection Act states that anyone who processes personal information must comply with eight principles. These state that information must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with individuals' rights
- Secure
- Not transferred to other countries without adequate protection

Appendix 1

Being open about how we will use information that individuals/organisations give us
The Data Protection Act says that we need to explain to people how we will use the personal information they give us. PFG also desires to be clear about how we will use organisational information which is supplied.

The following statement is a general explanation of how PFG will use information. This statement should be included on all forms, surveys, questionnaires and other documents where we ask for personal information.

If we are collecting information for a purpose that isn't included in this statement, we should amend the statement to make our full purpose clear.

How we use the information you give us:

Information you give PFG will be used by us to tell you about PFG services. PFG will communicate with you by telephone, letter, email, or in any other reasonable way. You can ask for a copy of the information we hold about you and your organisation, and if the

information isn't accurate, you can ask us to correct it. If you do not want to receive letters, emails and telephone calls from us in the future, please tell us in writing.

We will never pass your contact details on to salespeople, or to private organisations. If you do not want us to pass on your organisation's postal address, please let us know in writing.

We will use your information to report on the impact of peer support. This will be non identifiable case studies unless you expressly give consent and agree the finished case study.

Appendix 2

Dealing with disclosure

The Data Protection Act gives people rights to access personal information that organisations hold about them. This guidance explains what rights people have, and what are responsibilities are.

People have the right to know if we process (collect, store and use) their personal information.

People can ask us to tell them:

- What kinds of personal information we process
- How we use personal information
- Who we pass personal information on to, and in what circumstances
- People can also ask for a copy of the information records we hold about them, and for us to explain where we got our information from.
- If people want to get a copy of the information records we hold about them, they need to ask us in writing. We have to respond to written requests within 40 days.
- An individual only has the right to see personal information we hold about them personally no one can ask to see another person's information. If someone asks for a copy of their information record we need to check that they are the person the record is about.
- In some situations, by giving out information about one person, we may also give out information that makes other people personally identifiable. For example, our training records might show the names of everyone who attended a training course on a particular date. The Data Protection Act (Section 7, sub-sections 4-7) has special rules to say what should happen in these situations and we need to work in line with these rules.
- People can also ask in writing to be removed from our records, or to say how and when we can use the information we hold about them. For example, someone might choose not to receive emails from us, but might still want to receive the PFG newsletter. We need to deal with requests like this within 21 days.
- In general, all requests relating to the use, storing or deleting of records should be made in writing to the PFG Board.

Appendix 3

Passing on information

The PFG statement how we will use the information you give us explains that PFG will, in some circumstances, pass on contact information for organisations and individuals:
Information you give PFG will be used by us and our sponsors to tell you about PFG services. PFG will communicate with you by telephone, letter, email, or in any other reasonable way. You can ask for a copy of the information we hold about you and if the information isn't accurate, you can ask us to correct it. If you do not want to receive letters, emails and telephone calls from us in the future, please tell us in writing.

General Guidelines:

- PFG may pass contact information on to agents of the PFG to carry out a particular task (for example, asking volunteers to contact people on our database by telephone)
- PFG may not pass on contact information for organisations, individually or collectively, to private sector organisations wishing to sell services or goods
- PFG may not pass on information about an individuals' use of VAW services, without permission from that individual.

Appendix 4

Security

- Personal information relating to the involvement of individuals and organisations with PFG is stored centrally on the PFG database. This data is limited to contact information, details of individuals' use of PFG services, and details of individuals' mailing subscriptions. Data stored on the PFG database is not considered sensitive.
- Access to the database must be limited to current PFG staff and agents.
- Sensitive personal data must not be stored on the database (sensitive data includes information about an individuals' ethnicity, religion, sexuality or health, for example)
- The database is backed-up manually on a weekly basis. Automatic back-ups are run daily.
- Personal information relating to the recruitment and employment of PFG staff is stored securely in a locked personnel cabinet. This information is considered sensitive.
- Access to the personnel cabinet is limited to management staff.
- The key for the personnel cabinet is stored in a locked drawer.
- Before disposal, sensitive personnel documents are shredded.