DATA PROTECTION POLICY

1. INTRODUCTION

1.1 This is the People First (PF) policy about how, and why, we hold personal data about our members, employees, others who work or volunteer for us and our customers. This policy should be read in conjunction with the PF Confidentiality Policy.

1.2 This policy also outlines the approach taken by People First to ensure that it abides by all United Kingdom data protection legislation now and in the future. Data protection legislation means the General Data Protection Regulation (GDPR), the applied GDPR, the Data Protection Act 2018 (DPA),and any regulations made under the Act and regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive.

1.3 In accordance with the Data Protection (Charges and Information) Regulations 2018, PF is registered through the Information Commissioner's Office (ICO) which maintains a public register of organisations that process personal data.

1.4 Registration as a Data Controller requires us to provide certain information to the ICO, including:

- name and headquarters address
- types of personal data processed
- purposes for which the data is processed

1.5 PF is entered on the Data Protection Register reference number Z20622543 which is subject to annual review and update as required.

1.6 PF will always publish a privacy notice for clients and customers on its web sites and will also ensure that privacy notices for job applicants and employees are given as appropriate. These tell individuals what to expect of us when we collect and use their personal information and the legal bases we use to legitimise the processing. All privacy notices will be reviewed at the same time as the Data Protection Policy to ensure accuracy.

1.7 The GDPR introduces a duty to appoint a data protection officer (DPO) only if you are a public authority or body, or if you carry out certain types of processing activities. PF is not a public authority, however it does work on their behalf and so has appointed a DPO

to help it demonstrate compliance with legislation and be part of its focus on accountability. The DPO must be independent, an expert in data protection, adequately resourced, and will report to the Finance and Operations Director. The DPO can be an existing employee or externally appointed (current DPO is externally appointed) and will assist in monitoring internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority (ICO).

The DPO will help PF demonstrate compliance and be part of its enhanced focus on accountability.

2. DATA SUBJECTS

2.1 We collect, hold and process information consisting of personal data including sensitive personal data, now termed Special Category Data (see below) about all our employees, applicants for employment, self-employed contractors, agency workers and others who work with us, including members or volunteers, and for members of organisations and individuals who use our services. All identifiable individuals are referred to in legislation as "data subjects".

2.2 Staff and volunteers are informed during induction and/or at first point of contact with PF that their details are kept in accordance with the relevant legislation. They are held securely and confidentially, in line with the PF Record Retention Policy and the ICO Employment Practices Code. They are also informed that their details will not be passed on to another organisation without their prior consent unless there is a legal basis or statutory requirement to do so (e.g. HMRC). A members' register is maintained which is annually updated and the records of those who are no longer in membership deleted.

2.3 Customers who use PF services are also informed that their details are kept in accordance with the relevant legislation and that their details are held securely and confidentially for a specified period of time after the end of their PF intervention. This may be communicated to them in a number of ways:

- Verbally, at the first contact with a member of PF staff
- In writing including electronic media**.**

2.4 The purposes for which we hold any information about these data subjects include:

- administrative and personnel management purposes
- recruitment, appraisals, supervision, performance, promotion
- training, career development
- pay and remuneration
- pension and insurances and other benefits
- payroll, tax, national insurance, other deductions from pay, health and safety
- discipline and grievances
- to support customer interventions and advocacy services

- as intelligence about people's experience of health and care services
- research (e.g. commissioned reports for public authorities)
- management of contracted services
- company (Trust) administration

2.5 For each purpose where PF is the data controller it will determine at least one legal basis to legitimise the processing of general personal data and an additional legal basis where Special Category Data is processed.

2.6 Personal data relating to criminal convictions is governed by the Law Enforcement Directive (Part 3 of the DPA 2018) and this will be specified in privacy notices as appropriate.

2.7 Data subjects will be informed of the purposes and legal bases relevant to them in a privacy notice, together with other information classed as mandatory by the ICO.

3. RESPONSIBILITIES IN RELATION TO DATA PROTECTION

3.1 There are three levels of responsibility:

- The Board of Trustees and the Senior Leadership Team, lead by the Chief Executive (supported by the Appointed Data Protection Officer) who ensure overall organisational compliance.
- Department leads who ensure that their operational procedures comply with this policy
- All staff, volunteers, representatives and Board members who must comply with the operational procedures and ask for help if necessary

3.2 PF is committed to ensuring that all staff and volunteers understand their responsibilities under the GDPR and DPA. This will be done by ensuring that this Policy is received, read and understood by all staff and volunteers, and by providing appropriate training.

3.3 Where PF is a data processor, it is the responsibility of the data controller to determine the purpose/s for which the processing is done and determine the legal bases, or in exceptional circumstances to instruct PF to do this. In every case PF will do what the data controller instructs us to do as specified in a data processing agreement. PF will inform the data controller if a data subject contacts us to exercise one of their rights. All other obligations of a data processor are covered by this policy.

4. SPECIAL CATEGORIES OF PERSONAL DATA

4.1 The GDPR defines "special categories" of personal data to include information as to racial or ethnic origin, religious beliefs or other beliefs of a similar nature, membership of a trade

union, politics, genetics and biometrics (when used for ID purposes), health which may include learning difficulties, sex life or sexual orientation.
Special conditions apply for processing to reflect their sensitivity.

4.2 The purpose for which we hold special category personal data about data subjects is for the provision of specific services to individuals. Where data subjects are customers this is, for example, to keep an accurate record of past and to support continuing advocacy interventions. It may also include examples of experiences of health or social care services.

4.3 We may also process special category personal data about employees such as trade union membership, physical or mental health condition.

4.4 In addition to the above purposes, we may collect, hold and process data including special category personal data if it is necessary to do so for compliance with any statutory duty with which we are required to comply.

5 SUBJECT ACCESS REQUESTS

5.1 Data subjects have a right to access the data held about them by PF under the relevant legislation. Subject Access Requests can be made verbally or in writing to any representative of PF, who will then pass on the request to the Chief Executive, who will ensure that it will be responded to within one month – see Separate PF Subject Access Reques*t* Procedure**.**

5.2 To support the timely processing of Subject Access Requests, the Chief Executive will be responsible for ensuring that an up to date Register of Processing is maintained. Data Subjects will be asked in a request form to provide reasonable assistance to identify the information requested (e.g. date of contact and service type or location*).*

5.3 PF requires all employees and volunteers with access to personal information to ensure the need for confidentiality and to avoid improper use or transfer of such information as described in the Confidentiality Policy. Any employee who fails to adhere to these principles will render themselves liable to disciplinary action under PF's policies and procedures. If an employee or volunteer accesses staff or customer records without authority or as a requirement of their role, this is gross misconduct, which could lead to the summary termination of employment under PF disciplinary policies and procedures. In addition, such unauthorised access is also a criminal offence *w*hich may result in the prosecution of both the employee and PF in terms of S.170 of the Data Protection Act 2018.

6 DISCRETIONARY AND LEGALDISCLOSURE OF INFORMATION – (see also Confidentiality Policy)

6.1 Everyone using services provided by PF, and everyone working for PF has the right to expect that confidential information will only be used for the purpose for which it was given and will not be passed on to other people or agencies without that person's consent unless there is a duty to share or disclose under statutory powers which may include safeguarding processes.

6.2 Examples of disclosures which may be made under statute include but are not confined to:

- Child abuse will be reported to Children's Services, and/or the Police
- Safeguarding of vulnerable adults and children in line with the respective PF Safeguarding Polic*ies*
- Drug trafficking, money laundering, acts of terrorism will be disclosed to the police

6.2 In addition colleagues who believe an illegal act has taken place or that a service user or member is at risk of harming themselves or others, must report this to their line manager who will report it to the appropriate authorities.

6.3 Individuals will normally be informed of this disclosure.

7. RETENTION OF DATA

7.1 Please refer to the Record Keeping and Retention Policy.

7.2 PF will hold employee data in accordance with the The Employment Practices Code, issued by the Information Commissioner's Office.

8. ELECTRONIC COMMUNICATIONS

8.1 We have systems in place which allow us to monitor electronic communications by employees, including to websites, ensuring that these systems are being used in accordance with our Internet policies. The company also follows the guidance recommended by the Information Commissioners Office. This means that we:

- Pay particular attention to the risks of transmitting confidential employee or customer information by email
- Only transmit information between locations if a secure network or comparable arrangements are in place or ensure that all copies of emails received by managers are held securely
- Draw attention to the risks of sending confidential, personal information by email – when responding to other agencies encrypted e-mail will normally already be in place and must be used. Staff should seek advice from the Chief Executive's office in all other situations.

- Ensure that our information systems security policy, risk assessments and procedures including those of our data processors properly address the risks of processing personal information in all media and transmissions.

9 DATA BREACHES

PF as Data Controller is required by law to notify the Information Commissioner's Office (ICO) of any data breaches. Any employee, volunteer or member who becomes aware of, or suspects, that a breach has taken place (e.g. intentional or accidental disclosure of personal data to somebody who is not entitled to access it) must notify the Chief Executive or Finance and Operations Director or other member of the Senior Leadership team immediately. The Chief Executive, (supported by the appointed Data Protection Officer) will be responsible for notifying the ICO in the required format and for any necessary investigatory, mitigating or limiting action.

10. PRINCIPLES

10.1 The GDPR sets out six enforceable principles on which the full requirements of the law, incorporating the EU General Data Protection Regulation (GDPR), are based. *In* summary *t*hese principles are that data must be:

- Data processing must be lawful and fair
- The purposes of processing must be specified, explicit and legitimate
- Personal data must be adequate, relevant and not excessive
- Personal data must be accurate and kept up to date
- Personal data should be kept for no longer than is necessary
- Personal data shall be processed in a secure manner.

In addition Article 5 (2) requires that "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

10.2 The objective of this policy, supported by complementary policies and procedures in respect of confidentiality IT Acceptable Use and information systems security, is to ensure compliance.

11 FREEDOM OF INFORMATION ACT 2000 (FOIA)

11.1 Persons making Subject Access Requests commonly refer to their rights under "Freedom of Information". This Act covers **non** personally identifiable information not covered by other legislation. Where PF is the data controller, it is not subject to FOIA, but where PF is the data processor for a public body, or other organisation subject to FOIA, for example Healthwatch England, FOIA applies.

Any such Requests for Information must be referred immediately to the Chief Executive's Office so that they can be responded to within the twenty working days allowed.

12 NATIONAL DATA OPT-OUT

12.1 It is the duty of People First and People First Services including Healthwatch, as a provider for the local authority/authorities and the NHS to comply with the National data opt-out enabling clients to opt out from the use of their data for anything other than the services we provide.

12.2 If current uses or disclosures should have national data opt-outs applied, PF needs to:

- implement the technical solution as laid down by the NHS to enable us to check lists of NHS numbers against those with national data opt-outs registered
- have a process in place, when we get the results back, to ensure that we only use or disclose information for the returned list of NHS numbers, as any with national data opt-outs registered will have been removed

12.3 If we have no uses or disclosures which need to have national data opt-outs applied, we must still put procedures in place to assess future uses or disclosures against the national data opt-out operational policy guidance, and can choose to either:

- implement the technical solution in readiness, or
- be ready to implement it if needed for future data uses or disclosures

12.4 National data opt-outs apply to a disclosure when an organisation, for example a research body, confirms they have approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by another organisation responsible for the data (the data controller) such as an NHS Trust, or in this case PF/Healthwatch.

12.5 The CAG approval is also known as a section 251 approval and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002. The NHS Act 2006 and the Regulations enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed without the data controller being in breach of the common law duty of confidentiality.

12.6 In practice, this means that the organisation responsible for the information (the data controller) can, if they wish, disclose the information to the data applicant, for example a research body, without being in breach of the common law duty of confidentiality.

It is only in these cases where opt-outs apply.

12.7 Following careful scrutiny of the disclosures of relevant personal data which are made by PF, it has been determined that that the organisation does not currently have data disclosures which require opt-outs to be applied.

PF has chosen to be ready to implement the technical solution if needed for future data uses or disclosures.

12.8 Compliance still requires that PF/Healthwatch:

a. Ensures that there are procedures in place to apply the National data opt-out if at any time in the future this is required (only required if PF decides to be ready to implement)
b. Communicates the responsibilities of PF to employees, clients and partner organisations
c. Includes a statement on compliance with the National data opt-out on its website and in relevant privacy notices
d. Ensures that relevant printed materials on 'Your NHS Data Matters' are available in our public/communal spaces
e. Sets an official date for declaring compliance after ensuring that a., b., c. and d. are undertaken
f. Officially declares compliance

12.9 The official declaration of compliance is the 30th September 2021

Having due regard to ensuring that this is detailed in PF's relevant policies and procedures and that all employees are made aware of the requirement to comply and how this must be done, this means that PF is/will be compliant with Information Standard DCB3058 – Compliance with national data opt-outs.

Agreed by Trustees – October 2020
Updated by DPO – April 2021 due to Legislative changes.
Date for Review by DPO – October 2021