Data Policy

Responsible Director:	**Kellie Woodley**
Date of review:	**June 2025**
Next review date:	**June 2026**
Version:	**1.0**

Contents

Policy Statement

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. It also applies to The Well Communities and its data subjects

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 United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), and any regulations made under the Act.

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.

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

PF is entered on the Data Protection Register reference number Z20622543 which is subject to annual review and update as required. The registration number of The Well Communities is ZA276019.

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.

The UK GDPR introduces a duty to appoint a data protection officer (DPO) on

their behalf and so PF 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.

For People First this is Catherine Hunt (gdpr@wearepeoplefirst.co.uk).

1. Data Protection

1.1 Data Subjects

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".

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.

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

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

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.

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.

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.

1.2 Responsibilities in relation to data protection

There are three levels of responsibility:

- The Board of Trustees and the Senior Leadership Team, led by the Chief Executive (supported by the Appointed Data Protection Officer) ensure overall organisational compliance
- Department leads 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

PF is committed to ensuring that all staff and volunteers understand their responsibilities under the UK 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.

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.

1.3 Special categories of personal data

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 Request Procedure.

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 may 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).

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 which may result in the prosecution of both the employee and PF in terms of S.170 of the Data Protection Act 2018.

1.4 Discretionary and legal disclosure of information (Also see confidentiality policy)

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.

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 Policies
- Drug trafficking, money laundering, and acts of terrorism will be disclosed to the police

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.

Individuals will normally be informed of this disclosure.

1.5 Retention of data

Please refer to the Record Keeping and Retention Policy.

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

1.6 Electronic Communications

We have systems in place which allow us to monitor electronic communications by employees, including 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.

1.7 Data Breaches

PF as Data Controller is required by law to notify the Information Commissioner's Office (ICO) of certain 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 their line manager or Data Protection Officer immediately. The DPO, (supported by the appointed point of contacts within the Business team) will be responsible for notifying the ICO in the required format and for any necessary investigatory, mitigating or limiting action.

1.8 Principles

The UK GDPR sets out six enforceable principles on which the full requirements of the law, in summary these principles are:

- 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')."

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.

1.9 Freedom of Information Act 2000 (FOIA)

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.

1.10 National Data opt – out

It is the duty of People First, 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.

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
- 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

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.

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.

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.

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.

Compliance still requires 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

The official declaration of compliance was 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 compliant with Information Standard DCB3058 – Compliance with national data opt-outs.

2. Subject Access Request

2.1 Subject Access Request

This document sets out People First's (PF's) policy for responding to "subject access requests" under the Data Protection Act 2018 (DPA) and the United Kingdom General Data Protection Regulation (UK GDPR).

A subject access request (SAR) is a written or verbal request for personal information (known as personal data) held about an individual (data subject) by PF. The UK GDPR gives individuals the right to know what information PF holds about them. It provides a framework to ensure that personal information is handled properly. However, this right is subject to certain exemptions that are set out in the DPA.

A written or verbal request may be made to any employee or representative of PF. It is this individual's responsibility to pass it to the Chief Executive or, in their absence the Business Manager, immediately. and this will be covered in data protection training.

Data subjects will be informed of their right to make a subject access request in PF's privacy statements.

When we receive a subject access request we will first check that we have enough information to be sure of the data subject's identity. Often we will have no reason to doubt a person's identity, for example, if we have regularly corresponded with them. However, if we have good cause to doubt someone's identity we can ask them to provide any evidence we reasonably need to confirm it.

Where a subject access request is made for personal data that is being processed by PF on behalf of another organisation (that is, where PF is the data processor), PF will immediately inform the data controller of the request unless any agreement between the two parties specifies otherwise, and follow any instruction the data controller may give.

The DPA and UK GDPR do not stop you making a request on someone else's behalf. This is often necessary for a solicitor acting on behalf of a client, or it could simply be that an individual wants someone else to act for them. In these cases, the organisation will need to satisfy itself that the third party making the request has the individual's permission to act on their behalf. It is the third party's responsibility to provide this evidence, which could be a written authority to make the request, or a power of attorney. If a person does not have the mental capacity to manage their own affairs and you are their attorney, for

example you have a Lasting Power of Attorney with authority to manage their property and affairs, you will have the right to access information about the person you represent to help you carry out your role.

We will gather any manual or electronically held information (including emails) and identify any information provided by a third party or which identifies a third party. If we have identified information that relates to third parties, we may write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information unless the other party has provided their consent, or where comments have been made or professional opinions given by an employee whose employment contract specifies that such information may be made available to a data subject who makes a subject access request, in circumstances where the rights and freedoms of neither individual are compromised. If a third party objects to the information being disclosed we may seek legal advice on what we should do.

We have one calendar month starting from when we have received all the information necessary to identify the data subject, to identify the information requested, to provide the information or to provide an explanation about why we are unable to provide the information.

If no personal data is held about the person making the subject access request, they or their representative should be informed in writing immediately this has been ascertained.

In certain circumstances it may need extra time to consider a request, and we are allowed to take up to an extra two months. If this is likely, PF will let the data subject know within one month that it needs more time and why.

In many cases, it will be possible to respond in advance of the one calendar month target, and we will aim to do so where possible. Copies of the information will be sent in a permanent form. Wherever possible in a form requested by the data subject.

A copy of the personal data should be provided free of charge. PF may charge for additional copies or if we think the request is ‘manifestly unfounded or excessive’. If so, we may ask for a reasonable fee for administrative costs associated with the request. Any such reasoning will always be recorded.

2.2 Exemptions

The DPA contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. An example of an exemption is information covered by legal professional privilege.

If it is agreed that information is inaccurate, or there is some uncertainty, a note will be made of the error or alleged error and this will be kept on file together with the original information until such time as any legal or data protection issue is resolved, whether or not an exemption applies. Where it has been determined that information is inaccurate this can then be deleted from the file and only accurate data held.

2.3 Complaints

If a person is not satisfied by our actions, you can seek recourse through our internal complaints procedure.

If a person remains dissatisfied, you have the right to refer the matter to the Information Commissioner – https://ico.org.uk/for-the-public/personal-information/

3.Retention

3.1 Introduction

The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA) state that data should be kept no longer than necessary. This means that we must have a sound reason for keeping information and once we no longer need it we should securely erase or destroy it. All records are made and held in accordance with the data protection principles. It is People First's responsibility to ensure that their activities are compliant with the relevant legislation. Any data, whether held on computer systems or on paper, must be subject to a strict retention schedule.

Policy Statement

Accurate, proportionate records are kept in order to:

- Provide a high-quality service to customers and the public.
- Ensure that feedback can be provided.
- Ensure good support and supervision to staff and volunteers
- Comply with all employment, charity, and company legal requirements
- Comply with quality assurance systems.

Records are retained for the period specified in the procedure below, and with the exception of items that must be stored permanently, are then safely destroyed using the appropriate methods. The HR Officer is the named person responsible for this process.

3.2 Procedure

All paper-based records are held securely in a locked filing cabinet. Where possible such records are scanned and saved electronically.

Electronic files are kept securely, are password protected and regularly backed up. These include the database, payroll information, financial records, all HR records and retention records.

Data subjects are informed that personal information will be kept confidential and will not be shared with anyone other than third party providers (data processors) unless express consent has been given or there is a legal obligation to disclose it, for example where there is a safeguarding concern. When asking for consent to pass on personal details PF will always confirm how the information will be used and why it is passed on.

Stakeholder data held is reviewed and updated regularly, and no later than every 5 years.

Disclosure and Barring Scheme

When DBS checks are requested, PF will keep a record of the DBS reference number and the date the check was completed on the relevant volunteer or staff file, but does not keep a copy of the DBS check.

Retention Summary

PF complies with the requirements of company law and records are maintained and retained in accordance with the retention summary below. PF also complies with the Statement of Recommended Practice (SORP) in relation to its financial record keeping and reporting; and all financial records are retained in accordance with the retention summary below.

PF stores insurance policies and employer's liability insurance certificates and records relating to the ownership or leasehold of premises securely and in line with the retention summary below.

Retention Schedule

Employment Staff and volunteer records will be retained for six years after the end of employment, but should only contain sufficient information in order to provide a reference or if there is another legal basis for doing so. Copies of any reference given should be retained for 7 years after the reference request. Director's files should be retained for six years.	
Application form	Duration of employment, destroy when employment ends
References received	Duration of employment, destroy when employment ends
Sickness and maternity records Unpaid leave/special leave records	7 years from end of employment
Annual leave records	2 years after action completed
Records relating to an injury or accident at work	Retain Permanently
References given/information to enable a reference to be provided	7 years from date of reference
Recruitment and selection material (unsuccessful candidates)	Interview notes – 12 months following appointment
Appraisal records	7 years after employment has ended
Disciplinary records	7 years after employment has ended
Statutory maternity pay records, calculations and certificates	Retain while employed and for 7 years after employment has ended
Redundancy details, calculation of payments and refunds	7 years from date of redundancy

Note: if an allegation has been made about the member of staff, volunteer or trustee the staff record should be retained until they reach the normal retirement age or for ten years, if that is longer. E.g. around Safeguarding.

RECORD OF COMMENTS AND OTHER EVIDENCE	
Comments recorded on internal databases	6 years from end of service provision
Any paper based comments recorded on the database.	Destroy
Comments and or other evidence that have not been recorded on the database.	6 years from end of service provision
Signed consent forms recorded on internal database	6 years from end of service provision
Safeguarding Children	7 years after the child reaches 18 years old
Safeguarding Adults	6 years from end of service provision

FINANCIAL RECORDS	
Financial records	7 years – online only
Income tax and NI returns, income tax records and correspondence with HMRC	Three years after the end of the financial year to which they relate
Payroll records (also overtime, bonuses, expenses)	7 years – online only
Pension contribution records	7 years – online only
Pension scheme investment policies	12 years from any benefit payable under the policy
CORPORATE	
Employers liability certificate	40 years
Insurance policies	6 years
Certificate of incorporation	Permanently
Minutes of Board of Trustees	10 years

Memorandum of association	Original to be kept permanently
Articles of association	Original to be kept permanently
Variations to the governing Documents	Original to be kept permanently
Statutory registers	Permanently
Membership records	20 years from commencement of membership register
Rental or hire purchase agreements	6 years after expiry
OTHERS	
Deeds of title	Permanently
Leases	12 years after the lease has expired
Accident books	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).
Health and safety policy documents	3 years
Assessment of risks under health and safety legislation	3 years

4. Physical security

4.1 Introduction

The aim of this policy is to prevent unauthorised access to physical assets and electronic information. In summary, the policy requires the following to be protected:

- Sensitive paper records
- IT equipment

This protection may be as simple as a lock on a filing cabinet. The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. Each Department is responsible for assessing the level of protection required for their teams and locations.

All PF employees, volunteers, contractors, and users with access to PF equipment and information (electronic and paper records) are responsible for ensuring the safety and security of the equipment.

4.2 Scope

This policy applies to all users of PF owned, leased / hired facilities and equipment and all people who access our electronic and physical documents and information.

4.3 Secure areas

Critical or sensitive information must be stored in secure areas protected by appropriate security controls.

Physical security must begin with the building itself, and an assessment of perimeter vulnerability must be conducted. The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there, these could include:

- Alarms fitted and activated outside working hours
- Door locks
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be known only to those people authorised to access the area / building)
- CCTV cameras (Head office only)
- Protection against damage e.g. fire, flood, vandalism

Each staff member with the responsibility to open and close a People First office must ensure that doors and windows are properly secured at the end of the day.

Badges, keys, entry codes etc. must only be held by staff authorised to access those areas and should not be loaned / provided to anyone else.

Visitors are required to sign in and out with arrival and departure times.

Where breaches do occur or, a member of staff leaves outside normal termination circumstances keys, badges etc. should be recovered from the staff member and any door / access codes should be changed immediately, if required.

4.4 Paper based data security

Paper based (or similar non-electronic) information should be assigned to an owner. Paper in an open office must be protected by the controls for the building and other appropriate measures that could include:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area

4.5 Equipment security

All general computer equipment must be located in suitable physical locations that:

- Reduce risks from environmental hazards, for example, heat, fire, smoke, water, dust and vibration.
- Reduce the risk of theft.
- Facilitate workstations handling sensitive data being positioned to eliminate the risk of the data being seen by unauthorised people.

When using desktop PCs and laptops data must be stored on the OneDrive system. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All data is stored within the Microsoft Cloud system; this significantly reduces the risk of the operating system and data corruption from power failures. No changes can be made to the server specifications except by the IT Provider and not without consultation and authorisation from an internal IT member of staff and the Finance Director and/or the CEO.

All items of equipment should be recorded on an inventory. Procedures are in place to ensure inventories are updated as soon as assets are received or disposed of. A quarterly audit of People First “users” is also to be conducted as part of the process to ensure only active users are maintained and hold access to People First data. This will be conducted by the Business and Operations team.

4.6 Security of equipment off premises

The use of equipment is permitted following its correct and complete registration on the IT inventory and a signed Equipment Agreement by staff ensuring accountability for the equipment. Equipment taken away from PF premises is the responsibility of the user and must:

- Not be left unattended
- Be concealed whilst transporting
- Not left open to theft or damage whether in the office, during transit or at home
- Be encrypted if carrying personal or confidential information
- Be password protected
- Be adequately insured

Staff should be aware of their responsibilities regarding current Data Protection legislation.

4.7 Secure disposal or re-use of equipment

All IT equipment being disposed of must be done so through PF IT providers (David Allen IT)

- Equipment that is to be reused or disposed of must have all its data and software removed/destroyed. If the equipment is to be passed onto another organisation (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data-removing software tools.
- Software media must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

4.8 Policy compliance

If you are found to have breached this policy, you may be subject to the disciplinary procedure. If you have broken the law, you may be subject to prosecution.