

# SUBJECT ACCESS REQUEST POLICY

## 1. SUBJECT ACCESS REQUEST

- 1.1 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 General Data Protection Regulation (GDPR).
- 1.2 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 PFS. The GDPR gives individuals the right to know what information PFS 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.
- 1.3 A written or verbal request may be made to any employee or representative of PFS. It is this individual's responsibility to pass it to the Chief Executive or, in their absence the Finance and Operations Director, immediately, and this will be covered in data protection training.
- 1.4 The GDPR states that anyone who processes personal data must comply with six principles. In summary these are that personal data must be:
  - Processed fairly and lawfully
  - Processed for specified explicit and legitimate purposes
  - Adequate, relevant and not excessive
  - Accurate and kept up to date
  - Kept for no longer than is necessary
  - 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 the principles."

- 1.5 The GDPR provides individuals with important rights, including the right to find out what personal data is held about them electronically and in certain paper records. Personal data means any information relating to an identified or identifiable natural person ('data subject'), will cover basic details and will include details such as name,

address, telephone number, and also information and opinions held about that person in files, etc.

- 1.6 Data subjects will be informed of their right to make a subject access request in PFS's privacy statements.
- 1.7 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.
- 1.8 Where a subject access request is made for personal data that is being processed by PFS on behalf of another organisation (that is, where PFS is the data processor), PFS 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.
- 1.9 The DPA and 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.
- 1.10 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 will 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.
- 1.11 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.

- 1.12 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.
- 1.13 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, PFS will let the data subject know within one month that it needs more time and why.
- 1.14 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.
- 1.15 A copy of the personal data should be provided free of charge. PFS 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. EXEMPTIONS**

- 2.1 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.
- 2.2 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.

## **3. COMPLAINTS**

- 3.1 If you are not satisfied by our actions, you can seek recourse through our internal complaints procedure.
- 3.2 If you remain dissatisfied, you have the right to refer the matter to the Information Commissioner – <https://ico.org.uk/for-the-public/personal-information/>

**Agreed by Trustees – October 2020**

**Review date by the DPO – October 2021**