CONFIDENTIALITY POLICY

1. INTRODUCTION

1.1 This policy sets out People First Independent Advocacy's (PFIA) approach to the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR)and all other aspects of confidentiality as described in 1.2 below. The overall purpose of this policy is to ensure confidentiality in respect of all information relating to PFIA, employees, volunteers, representatives, Board members, and customers.

1.2 The organisation's confidentiality practices and procedures are underpinned by best practice, common law and legislation including Article 8 of the Human Rights Act, and it should be understood that breaches of this policy could result in disciplinary action as well as legal action being taken against responsible individual members of staff or PFIA as an organisation.

1.3 PFIA is committed to act responsibly and with integrity when handling personal information and data.

1.4 In complying with this policy all personal and sensitive information will be treated as confidential. No information will be disclosed without the prior informed consent of the individual concerned, except in the circumstances detailed in section 6 or where otherwise permitted by the law and where it does not affect the rights and freedoms of the individual and no attempt will be made to gain access to information that has not been authorised.

This policy should be read in conjunction with the Data Protection Policy. This contains a more detailed statement of policy and practice which apply to PFIA and its staff to ensure compliance.

2. CONFIDENTIAL INFORMATION

2.1 Confidential information is information entrusted by an individual *or* organisation in confidence, where there is general obligation not to disclose that information without consent or where there is another legal basis to do so.

2.2 Confidential information may include personal information such as name, age, address, and personal contact details and circumstances, as well as sensitive personal information regarding race, health, sexuality, criminal records, etc.

2.3 This policy also covers personal salary and expense details, supervision/appraisal/disciplinary/training records and other work related issues as well as home addresses and personal telephone numbers.

2.4 It also may cover sensitive customer or employee information, i.e. it involves disputes or legal issues, which will be confidential to the employee dealing with the situation and their line manager. Such information should be clearly labelled 'Confidential'.

2.5 Confidential information may be known, or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

2.6 Information that identifies individuals personally is assumed to be confidential, and should not be used unless absolutely necessary. Whenever possible, anonymised or pseudonymised data (from which personal details have been removed and which therefore cannot identify the individual) should be used instead. Note however that even anonymised information cannot be used without permission.

2.7 Confidential information should only be kept as required and for specific purposes. It must be relevant, up-to-date, accurate and not excessive for that purpose and will be accessible only to those members of staff that require the information in the performance of their duties.

3. WHY INFORMATION IS HELD

3.1 Information is held by PFIA relating to members, advocacy partners, voluntary and community organisations, self-help groups, volunteers, students, employees, directors or services which support or fund them.

3.2 Information is also held following engagement or survey activity and used to contribute to an evidence base and/or develop reports.

3.3 Some information is kept to enable PFIA colleagues to understand the history and activities of individuals and organisations in order to deliver the most appropriate support.

3.4 Information about ethnicity and disability of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

4. STORING AND DISPOSING OF CONFIDENTIAL INFORMATION

4.1 PFIA recognises that confidential information is gained about individuals and organisations during the course of its work or activities.

4.2 In most cases information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential.

4.3 General non-confidential information about organisations is kept in unlocked filing cabinets and on the Company Shared Drive (Z) with open access to all People First colleagues.

4.4 Information about volunteers, students and other individuals will be kept in lockable filing cabinets and in an appropriate folder on the Company Shared Drive by the colleague directly responsible. These colleagues must ensure line managers know how to gain access.

4.5 Employees' personnel information will be kept in a lockable filing cabinet by line managers and will be accessible to the Chief Executive. It is also kept on the SAGE online data storage system.

4.6 Application forms and supporting information are to be treated as strictly confidential and are to be kept in a secure place out of general view. Special care should be taken with information printed from the computer.

4.7 Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.

4.8 The advocacy database ensures information is retained online confidentially for the length of time specified in our Privacy Notices/Document Retention Schedule, through utilisation of several security levels, including staff passwords.

4.9 In an emergency situation, the Chief Executive may authorise access to files by other people.

4.10 No personal or business information held by PFIA should be kept on devices other than those listed in this policy.

4.11 Timely and secure disposal of information, both paper and electronic, including all manual records, printed documents and handwritten notes is carried out in accordance with data protection legislation.

4.12 Routine paper waste i.e. blank forms, early drafts of non-sensitive work, publicity material and "junk" mail should be put in the office paper recycling bin.

4.13 Any material that contains personal data about staff or customers must be disposed of via shredding where possible. Particular care must be taken with:

- Any material that contains Special Category personal data i.e. health issues, racial or ethnic origin, political opinions or trade union membership, religious or similar beliefs.

- Other significant personal data that refers e.g. to staff performance measuring or grievance or complaint matters

4.14 Each office has a shredder and confidential waste should be shredded as soon as practical. Confidential shredding must be supervised to ensure all documents are shredded securely and must not be left unattended.

4.15 We do not encourage staff to work from home, however should this be appropriate staff must not take any paperwork which is sensitive or classed as Special Category

personal data home unless absolutely necessary and must not dispose of any paper records containing personal or sensitive data in domestic waste. All such paper records must be returned securely to the place of work and disposed of in accordance with the guidance above.

4.16 Permission may be given to photocopy information but the process will be supervised.

4.17 Staff must not transfer confidential company information or personal identifiable information onto devices unless authorised to do so. Encrypted memory sticks can be made available and must be used if transferring personal identifiable information or confidential company information.

5. ACCESS TO INFORMATION

5.1 Information that is confidential to PFIA as an organisation can be passed to colleagues, line managers or directors to ensure the best quality support is provided.

5.2 Under the GDPR, an individual is entitled to make a request verbally or in writing to view their personal data. This can be made to any employee or representative of PFIA, who will pass it on to Chief Executive. PFIA has a statutory duty to provide the individual with copies of the personal data within one month unless permitted grounds for extension or exemptions apply – see 5.3.

5.3 There are some exceptions to an individual's right of access to personal data. This might include third party information on their data which should be redacted or permission sought from the third party to disclose or an exemption might apply. When this happens it should be carried out in accordance with data protection legislation and the PFIA Data Protection policy which includes subject access to records. In normal circumstances no fee will apply.

5.4 Employees, former applicants, volunteers, Board members and Trustees of PFIA also have a right to make a subject access request. The organisation will review information regularly to ensure record accuracy.

5.5 When photocopying or working on confidential documents, colleagues must ensure they are not seen by people in passing. This also applies to information on computer screens.

5.6 Colleagues should avoid talking about, individuals or organisations or in social settings. Please refer to the PFIA Social Media Policy for more information.

6. DISCRETIONARY AND LEGAL DISCLOSURE OF INFORMATION – see also Data Protection Policy

6.1 Everyone using services provided by PFIA, and everyone working for PFIA 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 under statutory powers and/or safeguarding procedures or another legal basis as specified in the GDPR.

6.1.1 Withdrawal of consent at any time may mean that an individual cannot access or otherwise benefit from the services provided by PFIA.

6.1.2 For persons who lack capacity to give consent to sensitive or confidential information being passed to other people or agencies are deemed as lacking capacity under the Care Act 2014 or Mental Capacity Act 2005. Information can be legally shared by following (section 4) the best interests principle.

6.2 It would not normally be expected that PFIA would discretionarily disclose any other confidential information.

6.3 There is a legal duty to disclose some information including:

- Child abuse will be reported to Children's Services, and or the Police
- Safeguarding of vulnerable adults in line with the PFIA Safeguarding Adults Policy
- Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police

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

6.5 Individuals will be informed of this disclosure, if following investigation a decision has been made to do so.

6.6 Where PFIA undertakes work on behalf of another organisation (the data controller) and is determined to be a data processor, PFIA will follow the instructions of the data controller regarding disclosure.

7. GENERAL DATA PROTECTION REGULATION (GDPR)

7.1 Information about individuals, whether on computer or on paper, falls within the scope of the DPA and GDPR and must comply with the data protection principles. In summary *t*hese 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."

8. BREACH OF CONFIDENTIALITY

8.1 Employees who are dissatisfied with the conduct or actions of other colleagues or People First should raise this with their line manager using the grievance procedure, if necessary, and not discuss their dissatisfaction outside People First.

8.2 Colleagues accessing unauthorised files or breaching confidentially may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

Agreed By Trustees – February 2019
Review date by DPO Catherine Hunt – October 2019