PRO-ACTION

Data Protection Policy

This policy applies to all employees and volunteers of Pro-Action.

Introduction

The purpose of this policy is to enable Pro-Action to:

- Comply with the law in respect of the data it holds about individuals.
- Follow good practice.
- Protect Pro-Action's clients, employees, volunteers, and other individuals
- Protect the organisation from the consequences of a breach of its responsibilities.

The Data Protection Acts 1998 & 2018

The Data Protection Acts give individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The 2018 Act was passed in May 2018 to bring the General Data Protection Regulations (GDPR) into legal force. This strengthens the protection of individuals' personal data and the processes required by organisations to meet the regulations.

The GDPR set out seven key principles that should lie at the heart of an organisation's approach to processing personal data:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The second area covered by the introduction of GDPR provides individuals with eight important rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Policy Statement

Pro-Action will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for processors i.e. employees and volunteers who handle personal data, so that they can act confidently and consistently

Pro-Action recognises that its first priority under the Data Protection Acts is to avoid causing harm to individuals. Information about any individual that we hold (see list of examples below) will be used fairly, securely, and not disclosed to any person unlawfully.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are considered. In addition to being open and transparent, Pro-Action will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Pro-Action is the Data Controller and is registered under the Data Protection Act 1998. All processing of personal data will be undertaken in accordance with the data protection principles.

Definitions

The Data Subject is the individual whose personal data is being processed. Examples include:

- Employees – current and past
- Volunteers
- Job applicants
- Donors
- Service users
- Suppliers.

Processing means the use made of personal data including:

- Obtaining and retrieving
- Holding and storing
- Making available within or outside the organisation
- Printing, sorting, matching, comparing, destroying.

The Data Controller is the legal 'person', or organisation, that decides why and how personal data is to be processed. The data controller is responsible for complying with the Data Protection Act.

The Data Processor - the data controller may get another organisation to be their data processor, in other words to process the data on their behalf. Data processors are not subject to the Data Protection Act. The responsibility of what is processed and how remains with the data controller. There should be a written contract with the data processor who must have appropriate security.

The Data Protection Officer is the name given to the person in organisations who is the central point of contact for all data compliance issues.

Responsibilities

Pro-Action's Board of Trustees recognises its overall responsibility for ensuring that Pro-Action complies with its legal obligations.

The Data Protection Officer is currently the Chief Operating Officer, who has the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other employees on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data

- Ensuring contracts with Data Processors have appropriate data protection clauses
- Electronic security
- Approving data protection-related statements on publicity materials and letters

Each employee and volunteer at Pro-Action who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed.

All employees and volunteers are required to read, understand, and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under Pro-Action's disciplinary procedures.

Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Any recorded information on members, learners, suppliers, volunteers, and employees will be:

- Kept in locked cabinets
- Protected by the use of passwords if kept on computer
- Destroyed confidentially if it is no longer needed

Access to information on the main database is controlled by a password and only those needing access are given the password. Employees and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

Notes regarding personal data of clients should be shredded or destroyed

Data Recording and Storage

Pro-Action stores data about members, partners, training delegates, funders and suppliers using the following methods:

- Xero UK Cloud Security that encrypts and backs up data using industry standard TLS (Transport Layer Security).
- Microsoft Cloud through OneDrive – check with Pete?
- Google Drive Account protected by using industry standard TLS (Transport Layer Security). Data is then unencrypted, then re-encrypt and backed up using AES encryption keys and stored in secure data centres. The cloud-based secure drive is password protected, with two-factor authentication and access is limited to key personnel.
- Extrapolated data from Google Drive is collated in password protected spreadsheets in order to provide services and reports to funders.

Pro-Action will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- Its systems are reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all employees and volunteers are forbidden from extrapolating additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information changes.
- Data will be corrected if shown to be inaccurate

Pro-Action stores historical archived paper records of service users, previous employees, and volunteers for a maximum of 7 years. Records are located in a locked storage facility with a three-factor authentication system and access is limited to key personnel.

There is an on-going programme of securely destroying paper records that are no longer required.

Access to Data

All clients and customers have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Officer within the required time limit.

Subject access requests must be in writing. All employees and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

All those making a subject access request will be asked to identify any other individuals who may also hold information about them, so that this data can be retrieved.

Where the individual making a subject access, request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

Pro-Action will provide details of information to service users who request it unless the information may cause harm to another person.

Employees have the right to access their file to ensure that information is being used fairly. If information held is inaccurate, the individual must notify the Chief Operating Officer so that this can be recorded on file.

Transparency

Pro-Action is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

Standard statements will be provided to employees for use on forms where data is collected. Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

Basis for gathering and holding personal data

Pro-Action has undertaken an assessment of all data it collects or may collect in the course of its activities, ensuring clarity of what is collected, why and under what basis, as well as how it will be used. Personal Data will be kept under different bases, depending on purpose e.g. Legitimate Interest for members, as they will expect to receive services and information from us.

Consent

Information about members and service users will only be made public with their consent. (This includes photographs.)

'Sensitive' data about members and service users will be held only with the knowledge and consent of the individual.

Consent may be obtained in various ways, in writing or online by an option to agree. For some services it is not always practicable to get consent in this way; in these cases, verbal consent will always be sought to the storing and processing of data. In all cases it will be documented that consent has been given.

Consent will not normally be sought for most processing of information about employees; however, employees' details will only be disclosed for purposes unrelated to their work for Pro-Action with express consent from the employee.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways, such as the right to opt out of direct marketing (see below).

Pro-Action acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where Pro-Action has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

For more specific guidance on employee responsibilities under data protection for service users please see Service User Data Protection Policy.

Direct Marketing

Pro-Action carries out very little direct marketing, and if so, only to those who have had previous contact with Pro-Action and who therefore would reasonably expect to receive information from us. In all cases we work to ensure that individuals have an option to unsubscribe. Most 'marketing' is to organisations within the children & youth sector of Hertfordshire that have a public profile and therefore have a shared interest in matters affecting/pertaining to children and young people.

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all Pro-Action marketing. Pro-Action does not have a policy of sharing lists, obtaining external lists, or carrying out joint or reciprocal mailings.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Employees training and acceptance of responsibilities

All employees who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process and the operational procedures for handling personal data. All employees will be expected to adhere to all these policies and procedures.

- Data Protection will be included in the induction training for all volunteers.
- Pro-Action will provide opportunities for employees to explore Data Protection issues through training, team meetings, and supervisions.

This policy has been ratified by the Pro-Action Board of Trustees and Chief Operating Officer.			
Signed:	**Position:**	**Name:**	**Date:**
T. Wilkins	Chief Operating Officer	Tracy Wilkins	17.07.2020