



DATA PROTECTION POLICY

A) INTRODUCTION

Croydon Voluntary Action is a membership organisation, set up to support local voluntary sector groups, social enterprises and active members of the community in their community work; this is clearly stated in our Constitution; it is in our legitimate interest to hold personal information to pursue our charitable objectives.

We may have to collect and use information about people with whom we work. These may include members, current, past and prospective employees, volunteers, clients, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the GDPR (General Data Protection Regulation) 2016 to ensure this.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We therefore ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the Principles of Data Protection as set out in the GDPR 2016.

1. The principles of data protection

Article 5 of the GDPR contains the principles and requires that personal data shall be:

- a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **“sensitive” personal data**.

For data to be classified under Personal Data, it must:

- a. Be data (so not unrecorded conversations with service users, donors or customers); and
- b. Be personal. Data is personal if it is concerned with identifiable, living individuals. It does not matter whether this data was processed automatically, electronically or manually. Personal data has been expanded to include IP addresses, internet cookies and biometrics, such as DNA and fingerprints.

Sensitive personal data is defined as personal data consisting of information as to:

- a. racial or ethnic origin;
- b. political opinion;
- c. religious or other beliefs;
- d. trade union membership;
- e. physical or mental health or condition;
- f. sexual life;
- g. criminal proceedings or convictions.
- h. Biometric Data and Genetic Data where processed to uniquely identify an individual (e.g. fingerprint payment systems)

2. Handling of personal/sensitive information

Through appropriate management and the use of strict criteria and controls, we make sure we:

- a. observe fully conditions regarding the fair collection and use of personal information;
- b. meet our legal obligations to specify the purpose for which information is used;
- c. collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- d. ensure the quality of information used;
- e. apply strict checks to determine the length of time information is held;
- f. hold accurate data that, where necessary, is kept up to date;
- g. shall not keep data for longer than is necessary for that purpose or those purposes;
- h. shall process data in accordance with the rights of data subjects under the Regulation;
- i. keep data secure i.e. protected by an appropriate degree of security;

In addition, we will ensure that:

- a. everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- b. methods of handling personal information are regularly assessed and evaluated;
- c. Permission is required for any recordings of meetings, whether in person or online and that the purpose of the recording is clear, transparent and agreed by participants. When no longer required, all recordings should be deleted.

All members of staff and volunteers are to be made fully aware of this policy and of their duties and responsibilities under the Regulations.

All managers, staff and volunteers must take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular ensure that:

- a. paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
-

-
- b. personal data held on computers and computer systems is protected by the use of secure passwords, which are systematically and regularly updated;
 - c. individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other agencies must:

- a. ensure that they and all of their staff who have access to personal data held or processed for or on behalf of us, are aware of this policy and are fully aware of their duties and responsibilities under the Regulations. Any breach of any provision of the Regulations will be deemed as being a breach of any contract between the Company and that individual, company, partner or firm;
- b. allow data protection audits by us of data held on our behalf (if requested);
- c. indemnify us against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors, consultants, partners or other agencies who are users of personal information supplied by us are required to confirm that they will abide by the requirements of the Regulations with regard to information supplied by us.

What do to in case of a data breach: the ICO, describes a personal data breach as “a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.” If a CVA employee or volunteer fears or discovers a personal data breach at CVA they should immediately notify the **Head of Communities**.

The Head of Communities will then:

- a. Notify the Data Subject without delay if the breach is likely to result in a high-risk activity (e.g., criminal activity such as fraud, or published in the public domain)
- b. Notify the Information Commissioner’s Office within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals. (This will be done at www.ico.org.uk/for-organisations/report-a-breach/)
- c. Notify the Charity Commission if any of the following applies:
 - i. Charity’s data has been accessed by an unknown person; this data was accessed and deleted, including the charity’s email account, donor names and addresses;
 - ii. A charity laptop, containing personal details of beneficiaries or staff, has been stolen or gone missing and it’s been reported to the police;
 - iii. Charity funds lost due to an online or telephone ‘phishing scam’, where trustees or signatories were conned into giving out bank account details;
 - iv. A Data Protection Act breach has occurred and been reported to the ICO.

3. Legal basis to process data

We believe CVA’s legal basis to process data about organisations’ employees, volunteers and members of the community under the GDPR 2016 is **Legitimate interest**. We applied a three steps test to arrive to this conclusion

- I. CVA is a membership organisation, set up to support local voluntary sector groups, social enterprises and active members of the community in their community work; this is clearly stated in our Constitution; it is in our legitimate interest to hold personal information to pursue our charitable objectives.
 - II. Is it necessary or can we do it in a different way?
 - a. CVA collects information on individuals working or volunteering for local community groups/social enterprises and community activists to be able to deliver its services to them. We would not be able to deliver our services otherwise.
 - b. CVA collects personal details of local residents who want to volunteer to be able to search for appropriate volunteering opportunities for them and
-

all the information we ask is necessary to deliver such service.

- c. CVA holds personal details of our own CVA volunteers. All volunteers' data will be held under the legitimate interest legal basis as we use volunteers to pursue our charitable objects.
- d. CVA collects personal details of active residents who want to engage with our community involvement projects.
- e. CVA collects basic contact details of residents asking to access our Food Hub.
- f. CVA has access to personal details of residents through its Social prescribing work but such data is held on Public Health's systems, for example EMIS.
- g. CVA holds personal details of employees and CVA volunteers under Legitimate interest under the GDPR 2016, as it is essential we have a way to contact them, or their next of kin, outside work in case of an emergency.

- III. Are we doing things that our members might object to? Are we intruding unfairly on an individual? We are clearly contacting members for provision of services only. As a membership organisation, those who come to us do so in order to access a service, which means we have a legitimate interest in processing their information.

CVA will be **transparent** about what we do with individual's data. We have a clear Privacy Notice for CVA members that is visible and accessible on our website which clearly states:

- Who we are and how to contact us;
- The purpose as well as the legal basis of the process – Why we require their information and how it is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- The legitimate interest – we are a membership organisation that provides services;
- Any overseas transfers – e.g. Mailchimp, Survey Monkey, Event Brite, Flickr and Better Impact. In all these cases individuals' information are held outside the EU;
- How long we hold data for;
- Individuals have right to access – this can include information held on emails;
- Individuals have the right to withdraw consent at any time – however this may not apply if it is in our legitimate interest;
- Individuals have the right to complain to the ICO;

Information on how employee's and volunteers' data is used is included in our Induction pack for new members.

A Privacy notice for CVA members is available on our website at [About us - Croydon Voluntary Action \(cvalive.org.uk\)](#)

A Privacy notice for residents wanting to volunteer through the Volunteer Centre can be found on our website at [Volunteer Centre Croydon Privacy Notice - Croydon Voluntary Action \(cvalive.org.uk\)](#)

A Privacy notice for residents involved in our ABCD (Asset Based Community Development) activities is available on 365 under Employee Information/Policies and Procedures and can be personalised and used by ABCD builders for their own area.

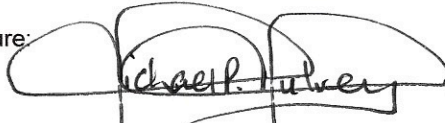
Reviewed: October 2021
Approved: December 2021

Approved for CVA
(Please PRINT)

Name: MICHAEL MULVEY
HONORARY TREASURER

Date: 20th December 2021

Signature:

A handwritten signature in black ink that reads "Michael Mulvey". The signature is written in a cursive style with a large, looped initial "M".

Date for review: December 2024
