THE CARES FAMILY

DATA PROTECTION POLICY

The Cares Family (including all local Cares Family branches) needs to gather and use certain Personal Information and special category data about individuals. This includes participants in our programmes and projects (older and younger neighbours), donors, fundraising partners, employees and other people The Cares Family needs to be in contact with. This data protection policy ensures that The Cares Family:

- ☐ Complies with data protection law and follows good practice;
- ☐ Protects the rights of staff, participants and partners;
- ☐ Is open about how it stores and processes individuals' data; and
- ☐ Protects itself from the risks of a data breach.

The Data Protection Officer for The Cares Family is: **Abbie Beckett, Operations Manager**

1. Data protection law

The Data Protection Act 1998, and the UK General Data Protection Regulation (UK GDPR) regulation all describe how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

1.1 Definitions

The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

If you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data.

1.2 Core Principles

The Cares Family is committed to ensuring it processes the information of neighbours, supporters and staff in accordance with the principles of the GDPR. We are required to ensure data meets the criteria below (examples given for each criterion):

1) processed lawfully, fairly and in a transparent manner in relation to individuals.

- Tell data subjects why you are collecting their information, what you are going to do with it and who you may share it with.
- e.g. when creating a mailing list remember to be open and transparent about what you will be doing with the information
- e.g. when working in a team, ensure that the older or younger neighbour is aware that all those involved with supporting them may need to see their notes.

2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

- Only use personal information for the purpose(s) for which it was obtained
- Only share information outside your team if it is appropriate and necessary to do so.

3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- Only collect and keep the information you require.
- It is not acceptable to hold information unless you can explain how it will be used e.g. taking both daytime and evening telephone numbers if you know you will only call in the day.

4) 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;

- Have processes in place to ensure information is accurate and up-to-date
- Ensure accuracy when inputting information
- Avoid creating duplicate records by checking existing records before creating new ones

5) 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;

- Follow records management retention guidance
- Ensure regular housekeeping/spring cleaning of your information
- Dispose of your information correctly

6) 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.

- Keep confidential papers locked away
- Ensure confidential conversations cannot be overheard
- Ensure information is transported securely
- Keep passwords secret

In addition, organisations are required to be **7) accountable, to be responsible for demonstrating compliance with data protection principles (e.g. publishing a Privacy Policy).**

2. The Cares Family responsibilities

We hold a limited amount of data about employees. We apply the same principles and rigour to the personal data we hold on employees and employees have the right to request access to it and its deletion. In order for an employee to be permitted to provide services to our neighbours, we are required to hold some of this data and as such refusal to allow us to do so may mean that an employee cannot work with us. In addition, notwithstanding a request for deletion, if an employee has worked with our neighbours, we need to retain certain personal information (notably your name and contact details) in the event an issue arises in the future. Again this information will only be stored for as long as we deem it reasonable.

- We shall retain a register of the systems used to access, store and protect data and this shall be reviewed annually.
- All staff will undergo GDPR training within their probation period and undertake annual refresher training.
- We will include a data protection checklist to our process for staff leaving the organisation to ensure their access to any personal information is revoked
- We shall perform an annual risk review and maintain data subject access and incident response processes as outlined in The Cares Family's Data Protection Procedures.
- We will perform a regular review of the data stored on the systems to ensure it is accurate and used in relation to the purposes for which it was captured and processed.
- Access to personal data shall be limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information. When personal data is deleted, this will be done so that the data is irrecoverable. Appropriate back-up and disaster recovery solutions shall also be put in place.
- In the event of a breach of security leading to the loss or unauthorised disclosure of, or access to, our participants' personal data, we shall promptly assess the risk to our neighbours' rights and freedoms and if appropriate report this to the appropriate authorities (more information available on the ICO website).
- We shall ensure there is a confidentiality clause in employment contracts and with any third party contractors

3. Staff Responsibilities

When starting work with a neighbour, you should ensure they are aware that we store their data in order to provide our support to them and we ask them to confirm that they permit us to store and use their personal data in this way. We will also explain to them the circumstances in which their data will be shared within the organisation. If they do not consent, then that may impact on our ability to support them – you should contact your manager to discuss if / how we can support the neighbour without access to their data. Where practical, we shall provide them with a copy of our Neighbour Data Protection Policy.

When capturing data of a supporter or donor it is important to ensure they are aware we will store their data in order to deliver our fundraising activity. If we want to communicate with them about future events or fundraising activity it is important we have captured their consent to do this and that all communications include an opportunity to unsubscribe. Consent must be logged onto the CRM.

3.1 Data storage

Everyone who works for The Cares Family has some responsibility for ensuring data is collected, stored and handled appropriately. In order for The Cares Family to work effectively

with neighbours and other stakeholders, it is necessary for us to collect and store information about them.

As a staff member of The Cares Family, it is crucial that you understand and comply with this policy to ensure we protect our neighbours. This policy applies to all data that we hold relating to identifiable individuals: names, addresses, email addresses, phone numbers and any other information relating to individuals. More information can be found in our Data Retention Policy.

- You must ensure that your laptop, phone and other hardware have active encryption. Use strong passwords. All computers should be protected by a firewall and software updates should be applied to your laptop when available. The Cares Family will ensure that you have access to the software and expertise necessary to achieve this.
- Data should be backed up frequently on the central IT systems and should not be saved directly on laptops.
- Data on our neighbours, donors and supporters should be stored on the secure CRM, Salesforce. Any data exported from the CRM should be anonymised if possible, stored securely and should be deleted after use.
- Any personal data that is not stored on the CRM should be password protected.
- No personal information of our neighbours should be stored on personal items of technology – this includes your personal laptop. If you use your laptop to capture information during a meeting with a neighbour then you should as soon as possible download the data to the central IT system and delete the local copy from your laptop.
- Where you print any data or make notes with pen and paper, you should make sure they are not left where unauthorised people could see them.
- As soon as possible, you should transfer any notes onto The Cares Family systems and carefully destroy the notes to avoid accidental disclosure. Printouts containing personal information should be minimised shredded and disposed of securely when no longer required.
- When you stop working with The Cares Family, you should no longer access our shared files, records, social media channels and documents.

3.2 Data sharing

- No data will be shared with any external organisation save in the following circumstances:
    i. Where it is our legal obligation to do so
    ii. Where it relates to an individual, you may share information with the notifying organisation (i.e. the organisation that told us about the neighbour) and other supporting bodies where it is reasonable and necessary to do so for the benefit of the neighbour. If you have any doubts, you must discuss and get agreement from your manager before sharing any information, or
    iii. Where the sharing of information relates to more than one individual, you must get the agreement of your manager. If The Cares Family has not previously dealt with the external organisation and / or the organisation is on a list where permission is required, the manager must get approval from the Board prior to sharing the information with said organisation.

4. Neighbour Data Protection: Our Use of Your Data

This following is our publicly stated commitment to participants in our core programmes:

In order to work with you, The Cares Family will occasionally need to gather and use certain personal information about you. For example, your name and address or other information pertinent to you (your “Personal Information”).

If you are providing information about other people you are responsible for, you must ensure you have their consent to share this information. By providing this information to us, we are entitled to assume you have that person’s permission to do so and for us to contact them.

Our primary concern is always the safety of our neighbours and volunteers. So if you have any concerns or issues with or about any other volunteer or neighbour with whom you interact as part of any The Cares Family’s activity, please do not hesitate to share those concerns and any further information necessary for us to take reasonable steps to protect or prevent any harm to any person.

This document details what we do with that information.

1. We collect your Personal Information in a number of ways, namely:
    a. When you complete a registration form in which you provide your name, address and contact details. For our volunteers we ask for additional personal information to allow us to complete appropriate digital screening checks;
    b. When you contact us either via telephone, email or via the website you will possibly be asked for the same information referred to above; or
    c. When you access our websites, we will collect, store and use information about the device used to access the website (please see our Cookie Policy at the foot of our website).
2. We only do this in order to engage you in The Cares Family’s activities and to manage and administer the support we provide. This may include sharing it with other institutions that support you (with your permission). For example, The Cares Family routinely shares your Personal Information between participants of the Love Your Neighbour programme in order for us to support you, but in sharing this data we shall ensure they will also comply with these rules.
3. We promise we never sell your Personal Information to any organisation.
4. We are required to ensure your Personal Information is accurate and so as part of our work, we may need to ask you some questions from time to time and sometimes even some we’ve asked you before.
5. If you are no longer engaging in The Cares Family’s work, we may keep your Personal Information in case you need our services again or for our records. You may ask us for a copy of what we hold about you or that we destroy our copy at any time by writing to us at The Cares Family, c/o 3Space, International House, Canterbury Crescent, Brixton, London SW9 7QE or by emailing us at info@thecaresfamily.org.uk and we will do as you ask. In addition, we will regularly review the information we hold and destroy those records for which we no longer have a good reason to store.
6. Your Personal Information is held electronically on our IT systems in a safe and secure way. Our staff will occasionally make notes in their notebooks, but they will then input any relevant data onto our IT system and destroy the paper copy – this is the best way to keep your Personal Information safe and secure.
7. The data that we collect from you may be transferred to, and stored at*, a destination outside the UK. It may also be processed by staff operating outside the UK who work for us or for one of our suppliers. We will take reasonable steps to ensure that your data is treated securely by any of our suppliers in accordance with this policy.*

8. *We ensure that all of our staff are aware of and adhere to these rules. If they leave us, they are not allowed to take any documentation or information about you with them.*
9. *In the event of a breach of security leading to the loss or unauthorised disclosure of, or access to, your Personal Information, we shall promptly assess the risk to your rights and freedoms and if appropriate report this to the appropriate Authorities (more information available here).*
10. *We will only share your personal information outside of The Cares Family if:*
    - *We have your consent to do so*
    - *There is a law which says we have to*
    - *If it is in the public interest, such as to prevent serious harm*

5. Data breaches and incident management

All breaches of data protection must be reported to the Data Protection Officer (named at the top of this policy). A personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data." (ICO)

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

Data breaches that pose a risk to the rights and freedoms of individuals may need to be reported to the Information Commissioner's Office, or in some instances to the Charity Commission. All reports should be made by the Data Protection Officer after assessing the level of the breach and the need to report it.

If data breaches pose a high risk to the rights and freedoms of individuals, they also need to be communicated to the individual(s) concerned directly. In assessing the risks, the following need to be considered:

- The type of breach e.g. there will be different consequences between whether data is lost compared to unauthorised disclosure;
- The nature, sensitivity and volume of personal data;
- Ease of identification of individuals;
- Severity of consequences: e.g. could the breach lead to fraud or theft, humiliation or reputational damage?
- Special characteristics of the individuals e.g. are vulnerable adults particularly affected?
- Number of affected individuals.

Breaches in confidentiality by staff will be managed through the disciplinary process.