GDPR: General Data Protection Regulations

Policy author	Fiona Rae
Policy creation date	18.12.20
Consultation period	09.02.21 – 26.02.21
Policy completion date	18.12.20
Review Date	**01.03.23**

1. PURPOSE

Community Food Initiatives North East (CFINE) is committed to the highest standards of openness, probity, and accountability.

2. APPLICATION

This procedure is applicable to all CFINE personnel, including volunteers.

3. RESPONSIBILITIES

Chief Executive Officer

The Chief Executive Officer (CEO) or person so designated by the CEO is responsible for General Data Protection Regulations.

4. PROCEDURE

4.1. What is GDPR?

The General Data Protection Regulation (GDPR) is a relatively new, Europe – wide law that replaced the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations need to handle personal data (from 25 May 2018).

4.2. Roles of Staff

All members of staff are responsible for ensuring GDPR and Data Protection issues are addressed, and regulations are adhered to.

Our Board of Trustees are responsible for overseeing data protection and privacy adherence by CFINE.

Data Controller – CFINE

Data Protection Risk Register – Fiona Rae, CEO

Data Protection Policy – Management Team

Data Subjects – Our staff, beneficiaries, volunteers, customers and supporters.

4.3. Collecting Data

All data stored on our system must be stored and used for its original purpose, and if this purpose changes, the person whose information we are storing should be notified.

We should not capture data that is not needed for processing. Only facts should be recorded, guesswork should not be recorded anywhere, unless it will be confirmed later.

Example data: Title, name, contact details, business information, connection to CFINE

Data collected should not be used for any reason other than the purpose it was gathered. Beneficiaries and volunteers should be given a privacy notice each time they are asked for information.

4.4. Privacy Notice

The Privacy notice should be easy to read and explain every aspect of data collection and use. People should be given notice of who will see their information, and how far it will be shared (only within CFINE unless we have permission otherwise). We must explain how sharing their data could affect them (i.e. they will receive information/campaigns/updates about CFINE).

Example:
Here at CFINE, we take your privacy seriously and will only use your personal information to contact you about our work, activities and updates, if you agree to receive this from us.

From time to time, we may contact you with information about the wider organisation, but we will never send you information which we do not think will interest you or affect you. If you consent to us contacting you for these purposes, please tick to say how you would like us to contact you:

Post □ *Email* □ *Telephone call* □ *SMS* □

We may work with third party companies on future projects, which would involve us temporarily sharing contact information with them for this purpose. These projects will always be managed by CFINE, and will always relate to our work. Your details will not be available to third parties on completion of the project. If you consent to us passing on your details for this purpose, please tick to confirm. I agree □

*Signature*_____ *Date*_____

You have the option to unsubscribe from our mailing lists at any time, just let us know by emailing info@cfine.org

4.5. Maintaining data accuracy & consent

Data should be cleansed and updated every two years to ensure that only valid and appropriate data is recorded. It should be clear to those who unsubscribe from communications with CFINE that their data is protected and know what will happen to it.

All information we hold should have consent attached to it, and this consent should be periodically updated and attached. Consent is only valid if it meets the existing standards and conditions of GDPR. (i.e. scanned and stored in a password protected folder)

Consent must be able to be **proven**, and **valid**, and **recorded**. We are responsible for keeping records stating that a person wishes for CFINE to contact them. This should be added to any application or registration forms or information gathering processes.

A 'database inventory' should be kept - information on who, when, how and what was consented should be recorded alongside a document showing their signature. This should be checked to ensure that what they consented to is still being honoured, and if purposes change, the individual should be notified, and a new consent obtained.

4.6. Access to information

CFINE colleagues should establish control procedures to limit access to information they obtain from people. Information individuals have given should only be available to employees who need this information to perform their jobs. Access to personal information – contact and financial – should be restricted and should not be accessible to people who do not need it. If employees change roles, access to this information should be adjusted as necessary. The use of personal devices with access to this information should be restricted to ensure security, integrity and confidentiality of personal data that people have shared in confidence.

CFINE examples of Legitimate Interest

Example	Legitimate Interest?
Contacting a pantry member with information about other services i.e. cooking classes.	Yes
Emailing a SAFE beneficiary to ask them to donate to CFINE.	No
Emailing a volunteer to inform them about fundraising activities.	Yes
Sending corporate partners our e-newsletter.	Yes
Sharing information about a beneficiary with another charity.	No – not without explicit permission. Or if they are at risk of harm
Contacting our former fundraisers with fundraising opportunities.	Yes
Maintaining a PR contact list.	Yes

Staff must	Staff must not
- Be open and transparent about why we are asking for information – if we can't be open and transparent, it is likely we don't need the data. - Keep records of contact, their consent responses and update information. - Adhere to the 'right to be forgotten' and archive their details to 'Anonymous' if they opt to no longer have their details on record.	- Contact anyone through a method of communication they have opted out from. - Assume that people will want to hear from us – if you are contacting them with 'legitimate interest' this must adhere to CFINE's definition of this - Don't ask for data that we don't need (age, gender) - Don't keep data without people's consent – add a disclosure on all documents asking for information. - Assume people want more information/thank you' s – they may have made a decision based on cost/environment as opposed to our message

4.7. Steps to GDPR & Data Protection compliance

1) Purpose

- Establish why we hold information and be able to explain with clarity how it will be used.
- Create an easy to read and understand Privacy notice for people to read when giving consent for use of their details.

2) Method

- Establish how data will be used to ensure that what we are recording and storing is appropriate and correct.
- If details will be passed onto other organisations, ensure that individuals know and that they have given consent for this.
- Define 'legitimate interest' in writing, with examples to ensure that we are adhering to this outline if making contact without consent.
- Prepare training for staff to ensure that they are aware and understand GDPR regulations, as well as data protection issues.

3) Lawfulness, Fairness and Transparency

- Make sure that our records show clearly that consent has been obtained

- Ensure that all individuals who we are contacting have agreed to be contacted, and have been given the option to opt-in to communications with CFINE.
- Ensure that all individuals know that they can, and know how to opt-out from communications at any point.
- Ensure everyone is aware of the new rights of the Data Subject;

    i. Right to Access – they can request what data, where and what it is being used for. This should be provided electronically free of charge,
    ii. Right to be forgotten – when consent is no longer given, and they request no further contact, an individual has the right to request their data and information be deleted.

- Create communication methods to obtain consent from individuals we are currently in touch with;
- Include privacy policy on all new communications with individuals;
- Include option to opt-out on all communications with individuals.