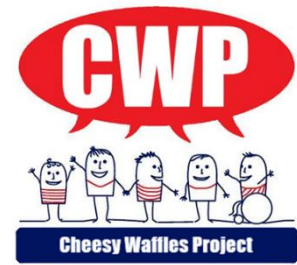


Cheesy Waffles Project

DATA PROTECTION POLICY



Part 1 Introduction and Key Definitions

Introduction

Cheesy Waffles Project need to gather and use certain information about individuals.

These individuals can include, members, parents/carers, staff, volunteers, trustees and other people the project has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the project's data protection standards – and to comply with the Law.

This data protection policy ensure Cheesy Waffles Project

- Complies with data protection law and follows good practice
- Protects the rights of members of staff, workers, volunteers, trustees
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

This Data Protection policy is based on the six principles of the Data Protection Act (DPA) that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. Accurate and kept up to date
5. Kept in a form which permits identification of data subjects for no longer than is necessary
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss or damage

Key Definitions

Data

The DPA describes how organisations, including Cheesy Waffles Project, must collect, handle and store personal information ('data').

Data is any information that the project collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data concerning health or sex life and sexual orientation;
- Genetic data; and
- Biometric data.

Data can be 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.

Data Subject

A 'Data Subject' is someone whose details the project keeps on file. The data subject has the following rights under data protection legislation;

- To be informed
- To have access to data stored about them (or their children)
- To rectification if there is an error on the data stored
- To erasure if there is no longer a need for the school to keep their data
- To restrict processing (e.g. limit what their data is used for)
- To object to data being shared or collected

Although data protection legislation affords these rights to individuals, in some cases the obligations the project has to share data with the DfE override these rights (this is documented later in the policy under 'Privacy Notices').

Data Controller

The management has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf.

The management are the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorized to collect or has already collected. It can be a member of staff, third party company or another organization such as the police or Local Authority (LA).

Part 2 Organisation Responsibility

Cheesy Waffles Project will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective. Trustees will be informed of any Data Protection incidents.

Roles and Responsibilities

The Trustees will:

- Establish and maintain a positive data protection culture.
- Ensure the Manager prepares a Data Protection policy for approval and adoption by the Trustees and to review and monitor the effectiveness of the policy.
- Allocate sufficient resources for data protection, e.g. in respect of training for staff etc.
- Monitor and review data protection issues.
- Ensure that the project provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.

The Manager will:

- Promote a positive data protection culture.
- Prepare a Data Protection policy for approval by the Trustees, revise as necessary and review on a regular basis, at least every two years.
- Ensure that all staff co-operate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the Officer to ensure they are fulfilling their responsibilities.
- Carry out a data protection induction for all staff and keep records of that induction.

Staff and Trustees at the project will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the project's data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the Project.

Part 3 Detailed Arrangements & Procedures

Data Protection Officer (Project Manager) Duties

- Inform and advise the project and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact
- Co-ordinate training on data protection

Data Protection Awareness

In order to ensure organisational compliance all staff, volunteers and trustees will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/trustee to the organization or if an individual changes role within the project.

Annual data protection refresher training will take place to reinforce the importance of staff adhering to the legislation.

A record of the professional development undertaken by the individual will be retained on their training record.

Consent

As a project, we will seek consent from staff, Trustees, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. Consent is defined by the PDA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

We may seek consent from young people also, and this will be dependent on the and the reason for processing.

The Use of Project Member Images

The Project takes photographs of its members which are used for internal displays, printed publications, project website or our social media accounts.

Cheesy Waffles project will seek consent from all parents/carers to allow the photography of members and the subsequent reproduction of these images. Consent will be sought on an annual basis.

Parents are given the opportunity to opt in. It is not permissible to assume parents are opting in.

Generic consent for all uses of images is not acceptable; parents/carers must give consent to each medium.

Parents/carers must be given the opportunity to withdraw their consent at any time. This should be given in writing to the project, however a verbal withdrawal of consent is also valid and should be reported to the key worker immediately.

If images on individual project members are published, then the name of that member should not be used in the accompanying text or caption unless specific consent has been obtained from the parent/carer prior to publication.

Accurate Data

The project will endeavour to ensure that the data it stores is accurate and up to date.

When a project member or member of staff joins the project they will be asked to complete a form providing their personal contact information (i.e name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the project will also seek consent to use the information provided for other internal purposes (such as promoting project events, photography).

The project will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the project to use the information held for internal purposes.

Parents/carers and staff are requested to inform the project when their personal information changes.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints.

Parents/carers and staff are requested to complete a Withdrawal of Consent form and return this to the Manager

Complaints

Complaints will be dealt with in accordance with the project's Complaints Procedure.

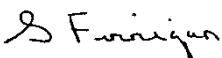
Data Breaches

Although the project takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use.
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood.
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the project

Subject Access Request

Any individual, person with parental/carer responsibility or project member with sufficient capacity has the right to ask what data the project holds about them.

Signed: 

Date: 19th April 2023

Susan Finnigan (Secretary/Trustee)

Signed: 

Date: 19th April 2023

Linda Pennington (Treasurer/Trustee)