Kids Kitchen
Cook delicious food together

Kids Kitchen Collective CIC
Data Protection Statement

This statement sets out how our work complies with the General Data Protecton Regulation (GDPR) and the UK Data Protection Act 2018.

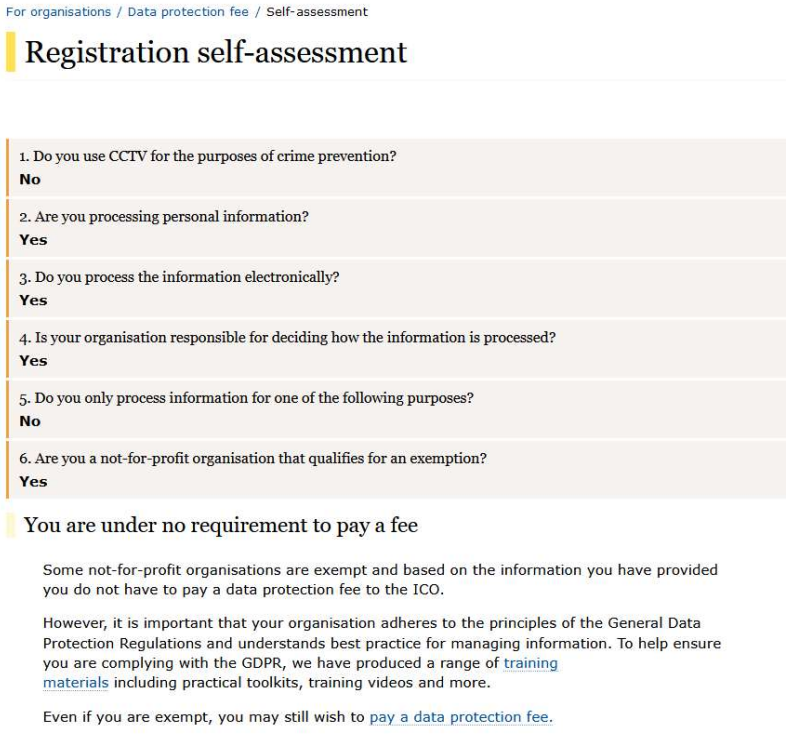
We are a Data Controller

We collect some personal data, and we decide when and how personal data is used.

We do not need to register as a Data Controller and do not need to pay a data protection fee.

We are a non- profit organisation that qualifies for an exemption. We:

- only process information necessary to establish or maintain membership or support
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- only hold information about individuals whose data we need to process for this exempt purpose
- the personal data we process is restricted to personal information that is necessary for this exempt purpose



For organisations / Data protection fee / Self-assessment

Registration self-assessment

1. Do you use CCTV for the purposes of crime prevention?
No

2. Are you processing personal information?
Yes

3. Do you process the information electronically?
Yes

4. Is your organisation responsible for deciding how the information is processed?
Yes

5. Do you only process information for one of the following purposes?
No

6. Are you a not-for-profit organisation that qualifies for an exemption?
Yes

You are under no requirement to pay a fee

Some not-for-profit organisations are exempt and based on the information you have provided you do not have to pay a data protection fee to the ICO.

However, it is important that your organisation adheres to the principles of the General Data Protection Regulations and understands best practice for managing information. To help ensure you are complying with the GDPR, we have produced a range of training materials including practical toolkits, training videos and more.

Even if you are exempt, you may still wish to pay a data protection fee.

We have a Record of Processing Activities (ROPA)

- A ROPA details the personal data we process and the reasons for this.
- Our team guidelines are informed by this record of all processing activities
- The ROPA is included with this statement.

We are not required to have a Data Protection Officer.

- Our core business activity is activities and events that build health, confidence and skills.
- During the course of that activity we collect some anecdotal evidence about the impact of what we do.
- Some of the data we collect is personal and concerns health. This is classed as special category data.
- We are not profiling people based on this personal information.
- Special category data is anonymised in order to report.
- Our work does not require regular, large scale processing or monitoring of individuals.

We have a lawful basis for processing (Article 6, UK GDPR):

- Consent has been given
- Processing is necessary for the performance of a contract
- We have a legitimate interest

Our conditions for processing special category data (Article 9 UK GDPR):

- We are a not-for-profit body and this data is collected in connection with the organisations' purposes. Data is not disclosed outside the organisation without the consent of the data subjects.

We have a Privacy and Cookie Notice.

We work with personal data, have a website, take photos at events and have a list of contacts.
The privacy notice covers the lawful basis for the personal data we collect, where it is stored and how we manage people's access to that data, including removal.
The cookie notice enables visitors to our website to opt out of unneccessary cookies.

We ask for consent to send emails.
Our contacts are individual subscribers and we ask for consent to send emails. We get this consent in paper form (session sign-up sheets) or through recording the date of sign-up in

our online mailing list. We make it clear on sign-up and every time we communicate that individuals can unsubscribe at any time.

We carry out Data Protection Impact Assessments
When starting new projects that ask for additional information not already included on our ROPA. A template follows this statement.

How we will complete a Data Subject Access Request:

- We don't receive any data that we don't collect ourselves.
- Our privacy notice notice makes it clear that people can make reasonable requests to rectify or remove data. We will do this by:
  - Removing information from monitoring spreadsheets
  - Blocking out names on scanned sign-in sheets
  - Removing from our booking system

Our team is aware of the law, and of how to work within the law to create impactful projects.

- We include this statement in our inductions for new regular workers and volunteers.
- We have a regularly reviewed **Data Protection How-To** on our Organisers Network including:
  - Don't keep sign in sheets after scanning in to evaluation online space
  - Online documents with personal data – keep password protected
  - Take steps to make all devices that have access to our online documents secure.
  - If a security breach occurs: You have 72 hours to do a ICO risk assesment for more action.
  - What to do if someone requests their information be removed

TEMPLATE: Data Protection Impact Assessment

This template is an example of how you can record your DPIA process and outcome. It follows the process set out by the the Information Commissioner's Office, in their DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

This should be used at the start of any major project involving the use of personal data, or if we are making a significant change to an existing process. The final outcomes should be integrated back into the project plan.

Submitting controller details

Name of controller – On behalf of Kids Kitchen

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA