DATA PROTECTION POLICY

AGREED- JULY 2023
REVIEW DATE- JULY 2024

Storing and processing personal information is necessary to Food Friends work. Food Friends recognise that personal information belongs to the person. Therefore, the Food Friends workforce must only use personal information in ways people expect and have consented to. Food Friends must also keep personal information safe and comply with the law.

The Food Friends team includes all Food Friends employees, trustees and volunteers.

Please find definitions of key words used in this policy in Appendix 2.

The Data Protection Act 1998

In 1998 the Data Protection Act was published. This is a law made to protect and keep personal information safe. It protects people's rights about the personal information that is kept by organisations such as Food Friends. The law applies to all the Food Friends team.

General Data Protection Regulations 2018 (GDPR)

The GDPR adds more to the requirements of the Data Protection Act. There are new responsibilities for organisations, such as Food Friends, that process personal information (personal data). These include:

- Stronger requirements for consent from people for their personal data to be stored and processed.
- The right to be forgotten. This means all personal data is deleted.
- Taking an approach to projects that promotes privacy and data protection compliance from the start and using privacy impact assessments to identify and reduce risk.
- A procedure allowing people to ask for access to data held about them that gives the individual stronger rights.
- If there is a breach of GDPR there are new, stricter requirements to notify the Information Commissioner's Office and the affected data subjects.
- A non-EU company could be subject to the same sanctions as EU companies.

How Food Friends meets the Data Protection Act (DPA) and GDPR

There are eight things the Data Protection Act says people and organisations must do.

To meet these, Food Friends will:

- Only process information for lawful reasons. People will be told why their information is being processed.
- Take enough detail for the information to be useful, but not more than required.
- Work with and support people to make sure that information is correct and up to date. People must tell Food Friends if their information changes or needs updating.
- Only keep information for as long as it is needed.
- Use information with the rights of the person in mind.
- Keep information safe
- Only send information to countries that have safe ways of working and can protect the information.

Roles and responsibilities

Responsibilities in governance and management

The Food Friends board is responsible for making sure all Food Friends projects comply with Data Protection laws and regulations, and with this Data Protection Policy.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for making sure all our work complies with this policy, monitoring Food Friends compliance with Data Protection law and regulation, and supporting everyone in Food Friends to work to the highest standards of Data Protection.

The DPO will provide a report every year to the trustee board and advise them on relevant data protection issues.

The DPO is the first point of contact for individuals whose data Food Friends processes. The DPO can be contacted using our central phone number or by email at hello@food-friends.co.uk.

The Food Friends DPO is currently Anna Mantell CEO

The workforce

Everyone in the Food Friends workforce is responsible for:

- Collecting, storing and processing personal data in accordance with this policy.

- Informing Food Friends of any changes to their personal data, such as a change of address.

- Contacting the DPO in the following circumstances:

1. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

2. If they have any concerns that this policy is not being followed

3. If they are unsure whether or not they have a lawful basis to use personal data in a particular way

4. If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area

5. If there has been a data breach

6. Whenever they are engaging in a new activity that may affect the privacy rights of individuals

7. If they need help with any contracts or sharing personal data with third parties

Collecting personal data

Lawfulness, fairness and transparency

Food Friends will only process personal data where they have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. The data needs to be processed so that Food Friends can fulfil a contract with the individual, or the individual has asked Food Friends to take specific steps before entering into a contract
2. The data needs to be processed so that Food Friends can comply with a legal obligation
3. The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
4. The data needs to be processed so that Food Friends can perform a task in the public interest
5. The data needs to be processed for the legitimate interests of Food Friends or a third party, provided the individual's rights and freedoms are not overridden
6. The individual has freely given clear consent

For special categories of personal data (see definitions below), Food Friends will also meet one of the special category conditions for processing under data protection law:

- The individual has given explicit consent

- The data needs to be processed to perform or exercise obligations or rights in relation to

employment, social security or social protection law

- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, Food Friends will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever Food Friends first collect personal data directly from individuals, they will provide them with the relevant information required by data protection law.

Food Friends will always consider the fairness of data processing, ensuring that personal data is not handled in ways that individuals would not reasonably expect, or used in ways which have unjustified adverse effects on them.

Limitation, minimisation and accuracy

Food Friends will only collect personal data for specified explicit and legitimate reasons. These reasons will be explained to individuals when the data is first collected.

If Food Friends want to use personal data for reasons other than those given when it is first obtained, individuals concerned will be informed and consent sought where necessary.

Our team must only process personal data where it is necessary

Food Friends will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when Food Friends workforce no longer need the personal data they hold, they must ensure it is deleted or anonymised.

Sharing personal data - General policy

Food Friends will not normally share personal data with anyone else without consent, but there are certain circumstances where they may be required to do so.

These include, but are not limited to, situations where:

- There is an issue with someone Food Friends support and/or their families that puts the safety of the workforce at risk
- There is a need to liaise with other agencies – consent will be sought as necessary before doing this
- Suppliers or contractors need data to enable Food Friends to provide services to people they support. For example, IT companies. When doing this, Food Friends will:

    1. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protectionlaw
    2. Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    3. Only share data that the supplier or contractor needed to carry out their service

Food Friends will share personal data with law enforcement and government bodies where legally required to do so.

Food Friends may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects anyone Food Friends support, employees, trustees or volunteers.

Where personal data is transferred internationally, it will be done so in accordance with data protection law.

Sharing personal data - Safeguarding

Sharing the right information, at the right time, with the right people, is fundamental to good practice in safeguarding. This can be a complex and a difficult area of practice. Anyone in doubt about sharing

personal information for safeguarding purposes should consult the DPO and/or the Safeguarding Lead. The Food Friends team must always report safeguarding concerns in line with Food Friends Safeguarding Children and Adults at Risk Policy.

Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Food Friends holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but Food Friends may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If anyone receives a subject access request, in any form, they must immediately forward it to the DPO.

For full details of subject access rights and how to ask, please visit ico.org.uk/your-data-matters/your-right-of-access/

Responding to subject access requests

When responding to requests, Food Friends:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual they will comply within three months of receipt of the request, where a request is complex or numerous. The individual will be informed of this within one month, and explain why the extension is necessary

Food Friends may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of a person Food Friends support or another individual
- Would reveal that the person is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the person's best interests
- Would include another person's personal data that cannot be reasonably anonymised, and consent has not been given and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, Food Friends may refuse to act on it, or charge a reasonable fee to cover administrative costs. Account will be taken of whether the request is repetitive in nature when making this decision.

Where a request is refused, a reason will be given along with the right to complain to the ICO. An individual can also seek to enforce their subject access right through the courts.

Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when their data is collected, and how it is used and processed (see above), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask Food Friends to rectify, erase or restrict processing of their personal data (in certain circumstances)

- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If anyone in our workforce receives such a request, they must immediately forward it to the DPO.

Photographs and videos

As part of our activities, we may take photographs and record images of individuals within Food Friends.

Written consent will be obtained from parents/carers, or people aged 18 and over, for photographs and videos to be taken of young people and adults for communication, marketing and promotional materials (Appendix 1).

Where parental consent is required, it will be clearly explained how the photograph and/or video will be used to both the parent/carer and child.

Any photographs and videos taken by people at Food Friends events for their own personal use are not covered by data protection legislation. However, Food Friends will ask that photos or videos with other people they support are not shared publicly on social media for safeguarding reasons, unless all the relevant adults or parents/carers have agreed to this.

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video concerned will be deleted and not distributed any further.

Data protection in all Food Friends work

The CEO is responsible for putting measures in place to show that Food Friends has integrated data protection into all of data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see above)
- Completing data protection impact assessments where Food Friends processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of the Food Friends workforce on data protection law, this policy, any related policies and any other data protection matters. Keeping a record of attendance
- Regularly conducting reviews and audits to test Food Friends privacy measures and make sure they are compliant
- Appropriate safeguards being put in place if Food Friends transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of processing activities, including:

1. For the benefit of data subjects, making available the name and contact details of Food Friends, the DPO and all information they are required to share about how they use and process personal data (via privacy notices)
2. For all personal data that Food Friends hold, maintaining an internal record of the type of data, type of data subject, how and why the data is being used, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how the data is kept secure.

Data security and storage of records

Food Friends will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office or project site tables or desks, or left anywhere else where there is general access

- Where personal information needs to be taken off site, workforce members must notify their line manager when it is taken off site and when it is returned

- Passwords that are at least 10 characters long containing letters and numbers are used to access Food Friends computers, laptops and other electronic devices. Everyone in Food Friends is reminded that they should not reuse passwords from other sites.

- People Food Friends support, workforce members and volunteers who store personal information on their personal devices are expected to follow the same security procedures as for Food Friends-owned equipment.

- Where Food Friends need to share personal data with a third party, due diligence will be carried out and all reasonable steps taken to ensure it is stored securely and adequately protected

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where it cannot or does not need to be rectified or updated.

Personal data breaches

Everyone in the Food Friends workforce is responsible for minimising the possibility of personal data breaches.

In the unlikely event of a suspected data breach, the procedure set out in appendix 3 will be followed.

When appropriate, Food Friends will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person

- The theft of a Food Friends laptop containing non-encrypted personal data about people supported

Training

All workforce members and volunteers, including Board members and Supported Internship Management Committee members, are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or Food Friends processes make it necessary

APPENDIX 1

Photo Release Form for Minors (if under 18)

Food Friends has my permission to use my photograph publicly to promote the charity. I understand that the images may be used in print publications, online publications, presentations, websites, and social media. I also understand that no royalty, fee, or other compensation shall become payable to me by reason of such use.

Parent/Guardian's signature: _____Date_____

Parent/Guardian's Name: _____

Child's Name: _____

Photo Release Form for Adults

Food Friends has my permission to use my photograph publicly to promote the charity. I understand that the images may be used in print publications, online publications, presentations, websites, and social media. I also understand that no royalty fee or other compensation shall become payable to me by reason of such use.

Signature: _____Date_____

Name: _____

APPENDIX 2

Definition of key words in this policy

Personal data (information)

Details of a living person that could be used to identify them. It includes name, date of birth, National Insurance number, address and someone's opinions, e.g. appraisal feedback on how an employee has worked in their job.

Sensitive personal data (information)

This includes details of a person's political opinions, religious beliefs, trade union membership, physical or mental health condition, sexual life, criminal record.

Information Commissioner's Office (ICO)

The organisation in the Government that makes sure that the Data Protection Act is in place and working as it should.

Processed/processing

This is when information is collected, stored, updated or worked with in any way by people or the organisation.

Data subject

The person whose personal information is being processed.

Data processor

A person who processes personal information for the data controller.

Data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Appendix 3: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the workforce member or data processor must immediately notify the DPO.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the investigator will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Made available to unauthorized people in the event of a breach
- Altered
- Disclosed or made available where it should not have been

The DPO will alert Food Friends trustee board.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant workforce members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure).

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:

1. The categories and approximate number of individuals concerned
2. The categories and approximate number of personal data records concerned

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

A description, in clear and plain language, of the nature of the personal data breach

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

As above, any decision on whether to contact individuals will be documented by the DPO.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts relating to the breach
- Effects

- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

The DPO and trustee board will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Special category data (sensitive information) being disclosed via email (including safeguarding records)

- If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.