GM Freeze Information Assurance Policy

VERSION 1
Adopted 16 April 2015

1. Introduction

The purpose of this policy is to ensure that we gather, store and use information about our staff, board members, members, supporters and other individuals securely, fairly and legally.

2. Data Protection Act

2.1. The Data Protection Act 1998 (the Act) regulates how 'personal data' must be managed and gives individuals certain rights around the data that we hold about them

2.2. GM Freeze is registered with the Information Commissioner to process personal data. We are named as a data controller under the register kept by the Information Commissioner in accordance with section 19 of the Act.

2.3. Under the Act, personal data means any recorded information held by us and from which a living individual can be identified. It includes names, addresses, telephone numbers, email addresses, photographs of people and other personal details. It also includes any expression of opinion about a living individual or any indication of our intentions about that individual.

2.4. Under the Act, sensitive personal data means information relating to a person's racial or ethnic origin; their political opinions, religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed, disposal of such proceedings or the sentence of any court in such proceedings.

2.5. The Act states that data must be processed according to eight enforceable data protection principles, included as Appendix 1. There are different rules for personal data and sensitive personal data.

2.6. The Act gives individuals the right to:

2.6.1. obtain their personal information from us except in limited circumstances

2.6.2. ask us not to process personal data where it causes substantial unwarranted damage to them or anyone else

2.6.3. claim compensation from us for damage and distress caused by any breach of the Act

2.7. GM Freeze will maintain its registration as a Data Controller and comply with all requirements under the Data Protection Act.

3. **Personal data collected and held by GM Freeze**

3.1. GM Freeze collects personal data (including some sensitive personal data) from staff, board members, volunteers, members, supporters, mailing list members, petition/action signatories and enquirers. Data is collected via website sign-ups, email, telephone, hard copy sign-ups, written correspondence and face to face contact.

3.2. Whenever personal data is collected, GM Freeze will tell individuals how their data will be used. Wherever possible this will be built into standard text on any printed or electronic forms used to capture data. When individuals offer their personal data proactively we will inform them in our reply or acknowledgement how we will use their data.

3.3. GM Freeze will not sell, rent, distribute or otherwise make people's personal data available to any third party except where they have given us their permission to do so or where the law requires us to do so.

3.4. GM Freeze may, from time to time, use a third party or contractor (such as a mailing house) to process data on our behalf. In this instance we remain responsible for ensuring that data is processed in accordance with the Act and will follow the Information Commissioner's guidance on outsourcing. Specifically, any third party will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by us.

3.5. GM Freeze may, from time to time, work jointly with members or other organisations on activities that include the collection and storage of personal data. Before embarking on such a project (or as soon as it becomes clear that an activity may include such an element if this is later), we will agree an information assurance action plan with the other party/ies, including, but not limited to:

3.5.1. Clear shared understanding of who will be responsible for collecting and storing personal data and what procedures they have in place to ensure compliance with this policy.

3.5.2. Clear shared understanding of who will have access to personal data once the joint project or activity is complete and what procedures are in place to communicate this to data subjects.

4. **Keeping data secure and up to date**

4.1. Electronic files containing personal details will be encrypted with a password. Passwords will only be shared with staff, board members or volunteers who have completed a data protection induction and will never be communicated in a method that attaches them in any way to the data itself. For example, passwords must not be stated in emails to which data is attached.

4.2. Electronic files containing personal details will only be stored via online file sharing facilities once the Director is satisfied that adequate security measures have been put in place, either by the provider of the file sharing facility or by GM Freeze itself.

4.3. Hard copies of personal data will be stored securely. Where hard copies of personal data (such as sign-up sheets from events) need to be transferred from one location to another, this must be done in person or via a secure postal service.

4.4. We will take particular care not to accidentally disclose personal information, for example, when trying to match a telephone caller with data held electronically.

4.5. Email accounts which are used to receive, process or store personal data of any kind will be held securely. Access will only be given to staff, board members or volunteers who have completed the appropriate level of information assurance induction, as detailed under 6.2 or 6.3, below.

4.6. We will endeavour to keep personal data up to date, encouraging contacts to inform us of any changes and noting any such changes promptly. This includes cross-referencing where personal data about an individual is held in more than one place.

5. **Subject access**

5.1. Individuals (known in this context as data subjects) are entitled to see the information that we hold about them. This is often referred to as subject access. Individuals who make a written request and pay the appropriate fee are entitled to be:

5.1.1. Told where any of their personal data is being processed.

5.1.2. Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.

5.1.3. Given a copy of the information comprising the data; and given details of the source of the data (where this is available).

5.1.4. There are some exemptions, detailed on the Information Commissioner's Office website

5.2. The Act requires us to comply with any such request within 40 calendar days of receiving it. We will respond to all requests courteously and aim to comply within 20 calendar days of receiving the request.

5.3. We are entitled to charge a fee of up to £10. Our usual practice will be to charge the maximum fee but this may be waived at the discretion of the Director.

6. **Training and review**

GM Freeze will ensure that information assurance is prioritised in all interactions with individuals. In order to achieve this we will:

6.1. Regularly review our procedures for data collection and management.

6.2. Require all staff, board members and volunteers who may have any contact with personal data to read and confirm their understanding of this policy, including appendices.

6.3. Require all staff, board members and volunteers engaged in regular data collection or processing to read more detailed guidance published by the Information Commissioner's Office, view the commissioner's own training videos and discuss their contents with their manager to ensure that they have fully understood their responsibilities.

6.4. Review and update this policy at least every three years.

7. **Responsibility**

The Director is responsible for ensuring that this policy is effectively implemented.

Appendix 1: Data Protection Principles

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2[i] is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3[ii] is also met.

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

---

[i] Schedule 2 and Schedule 3 are not detailed in the Information Commissioner's Office guidance so the links above are to www.legislation.gov.uk where the versions included in the Data Protection Act 1998 and any later amendments are listed. It appears that a reasonable (relatively) plain English interpretation would be as follows.

Schedule 2 – for personal data

1. the individual has consented to the processing
2. the processing is necessary for the performance of a contract with the individual
3. the processing is required under a legal obligation (other than one imposed by a contract)
4. the processing is necessary to protect vital interests of the individual (ie in a life or death situation)
5. the processing is necessary to carry out public functions such as the administration of justice

6. the processing is necessary in order to pursue our legitimate interests or those of third parties (unless it could unjustifiably prejudice the interests of the individual)

[ii] **Schedule 3 – for sensitive personal data**

1. the individual has explicitly consented to the processing
2. we are required by law to process the information for employment purposes
3. we need to process the information in order to protect the vital interests of the individual or another person (ie in a life or death situation)
4. the processing in necessary to deal with the administration of justice or legal proceedings