Data Protection Policy

1. Policy statement

Computer Friendly (CF) is committed to ensuring that the personal information it holds is managed responsibly in accordance with relevant legislation.

All Computer Friendly trustees and volunteers must comply fully with this policy.

2. Scope and purpose

The purpose of this policy is to ensure that Computer Friendly complies with legislation when dealing with personal data in electronic or hard copy form. Computer Friendly commits to compliance with the:

- Data Protection Act 1998 and its successor the Data Protection Bill 2017
- General Data Protection Regulation 2016 (GDPR)
- Privacy and Electronic Communication Regulations 2003 (PECR)

3. Data Protection Acts

The Data Protection Act 1998 provides a framework for the handling of personal data, defined as data relating to an identifiable living individual. A fuller definition of 'personal data' and other terms used can be found at the end of this policy.

The Act provides eight principles. Personal data shall be:

1. Processed fairly and lawfully;
2. Obtained for specified and lawful purposes only and processed in accordance with those purposes;
3. Adequate, relevant and not excessive;
4. Accurate and kept up to date;
5. Not kept for longer than is necessary;
6. Processed in accordance with the rights of data subjects;
7. Kept secure; and
8. Transferred only if privacy is respected.

The 1998 Act is to be replaced by a Data Protection Bill 2017, due for enactment in 2017/2018, which provides new data protection standards based on the GDPR.

4. The General Data Protection Regulation 2016

The General Data Protection Regulation (GDPR) is an EU-wide price of legislation. It provides six principles similar to those of the DPA. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principles relating to individuals' rights and the overseas transfers of personal data are covered elsewhere in the GDPR.

The GDPR provides data subjects with the following rights:

1) The right to be informed
2) The right of access
3) The right to rectification
4) The right to erasure
5) The right to restrict processing
6) The right to data portability
7) The right to object
8) Rights in relation to automated decision making and profiling.

The GDPR adds to the DPA the principle of accountability. It requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." This means that records of compliance activities must be kept.

5. Privacy and Electronic Communications Regulations (PECR) 2003

The Privacy and Electronic Communications Regulations (PECR) give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and

- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

6. Responsibilities

The Computer Friendly Board of Trustees has overall responsibility for data protection in the organisation.

All trustees and volunteers have a duty of care towards for the personal information which they manage or have access to.

7. Personal data held by Computer Friendly

Computer Friendly holds personal data about

- its trustees, volunteers and applicants.
- Its supporters and benefactors
- its students

The data held may include some special category (sensitive) data such as health information in addition to ordinary personal data.

8. Collecting personal data

Computer Friendly's grounds for collecting data from applicants, volunteers and students are in GDPR terms based on 'legitimate interests' e.g.

- student data is collected in order to contact and provide a service to students and inform them of CF activities.
- trustee, volunteer and applicant data is collected in order to select suitable candidates and to contact them and keep them informed
- data for other contacts may be collected for marketing purposes

Consent will not be needed as a basis for processing. However, CF will collect only the personal data necessary for the purpose for which it is collected. Should CF wish to use data for another purpose, a statement to this effect will be included on the data collection form and the data subject will be given the opportunity to consent or refuse.

All forms collecting personal data, whether electronic or in paper format, will include a statement outlining who will use the data and what it will be used for. This includes forms for applicants, volunteers and students.

9. Managing personal data

Personal data will be stored securely:

- Trustees and volunteers will be responsible for ensuring that any personal information that is held by them is kept securely, either physically locked away or password protected, and is not disclosed, either orally or in writing, to any third party outside of a legal requirement or a need for data sharing agreed by trustees.
- CF computers and other devices holding personal data will be encrypted and at end of life disposed of using secure methods

- Personal data will not be downloaded onto personal laptops, memory sticks or other forms of removable media unless protected by encryption.

Computer Friendly will ensure that:

- Personal data will not be kept for longer than is necessary.
- Personal data will not be sold to any outside organisation.
- Personal data will only be shared with other organisations where necessary for its stated purposes and this sharing will be made explicit in consent clauses.
- Any new software or procedures will meet and support data protection requirements.

Records will be kept of compliance activities. These include:

- Data collection forms
- Disposal activities
- Policies and procedures
- The handling of subject rights.

10. Subject rights

The right to be informed is covered under Collecting Personal Data above.

Right of access

Computer Friendly will provide the data subject with the following information when requested:

- Whether CF holds any personal data relating to the enquirer
- A description of the data
- Why it is held and for what purpose and how long
- To whom it may be disclosed

A copy of the information held will also be provided subject to any exemptions in legislation. All requests for access must be made in writing. CF will comply with the request within one month.

Other rights

CF will comply with the data subject's right to require that data is rectified, restricted or erased. The request must be made in writing.

Data subjects will be removed from mailing lists upon request.

CF will not use automated decision making or profiling.

The service offered by CF is not fully provided elsewhere therefore the data portability right does not apply.

11. Procedures, communication and training

Computer Friendly will write data protection requirements into procedures for trustees and volunteers.

Data protection policy and procedures will be communicated to trustees and volunteers and those that are relevant to members of the public will be published on the CF web site.

Data protection policy and procedures will be included in training for trustees and volunteers.

12. Monitoring

Compliance with this policy and related procedures will be monitored by the Board of Trustees.

13. Policy Owner and Review

This policy is owned by the Board of Trustees.
This policy was last approved in November 2017.
The next date of review will be November 2018.

Appendix: Data Protection Definitions

Data	Any information which is being processed automatically or recorded in any format.
Personal data/ Information	Data which relates to a living individual who can be identified from that data or from that data and other information. Personal data includes any expression of opinion about the individual and any indication of the intentions of the data controller.
Data controller	The individual or organisation (in this case Computer Friendly) responsible for ensuring that the requirements of the data protection legislation are complied with.
Data subject	An individual who is the subject of personal data.
Sensitive data	DPA term for information about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed by him/her.
Special categories of personal data	GDPR equivalent of DPA sensitive data. Its term for information about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition or sexual life, or biometric or genetic data. Information about the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed by him/her, while not included in the GDPR 'special categories', should be treated with the same sensitivity.
Legitimate interests	According to recital 47 of the GDPR: (47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.