FROM Wales Charity Number 1149385

Data Protection Policy and Procedures

Introduction

We are committed to a policy of protecting the rights and privacy of individuals. FROM Wales needs to collect and use certain types of Data in order to carry on our work. This personal information must be collected and dealt with appropriately.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data).

Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The board, staff and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act.

Board members staff and volunteers who have access to personal information, will be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out FROM Wales commitment and procedures for protecting personal data. The board regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

The Data Protection Act

This contains 8 principles for processing personal data with which we must comply.

Personal data:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purpose specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3. Shall be adequate, relevant and not excessive in relation to those purpose(s),

4. Shall be accurate and, where necessary, kept up to date,

5. Shall not be kept for longer than is necessary,
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes an appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. 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 information.

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

Data Controller – The person who (either alone or with others) decides what personal information FROM Wales will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person on the management committee who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998.

Data Subject/Service User – The individual whose personal information is being held or processed by FROM Wales (for example: a service user or a supporter)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

Explicit consent is needed for processing sensitive data this includes the following:

1. (a) racial or ethnic origin of the data subject
2. (b) political opinions
3. (c) religious beliefs or other beliefs of a similar nature
4. (d) trade union membership
5. (e) physical or mental health or condition
6. (f) sexual orientation
7. (g) criminal record
8. (h) proceedings for any offence committed or alleged to have been committed

Notification – Notifying the Information Commissioners Office (ICO) about the data processing activities of FROM Wales. Note: Not-for-profit organisations are exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the Group.

Applying the Data Protection Act within the charity

Whilst access to personal information is limited to the staff and volunteers, Volunteers may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances, we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose. Written consent will be gained from each individual in this circumstance.

Correcting data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Responsibilities

FROM Wales is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

The management committee will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

1. a) Observe fully conditions regarding the fair collection and use of information.
2. b) Meet its legal obligations to specify the purposes for which information is used.

3. c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
4. d) Ensure the quality of information used.
5. e) Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
6. i) The right to be informed that processing is being undertaken ii) The right of access to one's personal information
   iii) The right to prevent processing in certain circumstances, and iv) The right to correct, rectify, block or erase information which is regarded as wrong information
7. f) Take appropriate technical and organisational security measures to safeguard personal information,
8. g) Ensure that personal information is not transferred abroad without suitable safeguards,
9. h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
10. i) Set out clear procedures for responding to requests for information.

The Data Protection Officer on the management committee is:

Name: Bethan Robinson

Contact Details: 07970102985

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

1. a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice
2. b) Everyone processing personal information is appropriately trained to do so
3. c) Everyone processing personal information is appropriately supervised
4. d) Anybody wanting to make enquiries about handling personal information knows what to do
5. e) Dealing promptly and courteously with any enquiries about handling personal information
6. f) Describe clearly how the charity handles personal information
7. g) Will regularly review and audit the ways it holds, manages and uses personal information
8. h) Will regularly assess and evaluate its methods and performance in relation to handling personal information

All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Data collection: Informed consent

Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.

We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, we will ensure that the Data Subject:

1. a) Clearly understands why the information is needed
2. b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
3. c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
4. d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
5. e) Has received sufficient information on why their data is needed and how it will be used

Procedures for Handling Data & Data Security

Under the data protection act 1998, companies and charities have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- unauthorised or unlawful processing of personal data
- unauthorised disclosure of personal data
- accidental loss of personal data

All staff must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or in a computer or recorded by some other means.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc.

would be classed as personal data, and falls within the scope of the data protection act.

It is therefore important the all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Operational Guidance

Email:

All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or, printed and stored securely. The original email should then be deleted from the personal mailbox and any "deleted items" box, either immediately or when it has ceased to be of use.

Remember, emails that contain personal information which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access.

Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program.

Ensure your laptop is locked (password protect) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of site, preferably in the boot.
If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable) or processed for safe storage or disposal.

Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

Passwords:

Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password:

- Common sense rules for passwords are: do not give out your password
- do not write your password somewhere on your laptop
- do not keep it written on something stored in the laptop case

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised volunteers.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is our responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

Information Regarding Employees or Former Employees

Information regarding an employee or a former employee or volunteer or trustee will be kept indefinitely. For example, A need to refer back to a job

application or other document to check what was disclosed at a specific time or circumstance.

Data Subject Access Requests

Members of the public may request certain information from public bodies under the Freedom of Information Act 2000. The Act does not apply to charities, but we are still required to respond to requests for information under the Data Protection laws.

Disclosure

We may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent.

These are:

1. a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person
2. b) The Data Subject has already made the information public
3. c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
4. d) Monitoring for equal opportunities purposes – i.e. race, disability or religion
5. e) Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

We intend to ensure that personal information is treated lawfully and correctly.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

Destroying personal data

Personal data should only be kept for as long as it is needed i.e. only keep that data for the duration of administering the campaign/project and securely dispose of once the promotion and monitoring period is complete. We will review the list annually, and will ensure that this information is confidentially destroyed at the end of the relevant retention period.

Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to the charity please contact the Data Protection Officer: Bethan Robinson 07970102985

The Information Commissioner's website (www.ico.gov.uk) is another source of useful information.