Data Protection Policy

The law tells us what we must do when we ask for and keep information about people.

The person in charge of looking after our information is **The Business and Finance Manager**

Revised January 2022

What type of information do we keep?

Information to run the organisation

We need information about:

- members
- Board members
- activities
- other organisations

We keep people's personal information. So we are registered with the Information Commissioner's Office.

We will keep information confidential.

Anyone can ask to see their own information.

We will share information with other people or organisations if the law says we must.

Information about staff

We keep records about all staff.
This is kept confidential.

How we will keep information safely

Asking people for information

When we ask people for information we will:

- say why we want to keep that information
- say how we will use it
- let them see what information we have about them
- tell them that we will:
    - keep the information safe
    - only let the people who need to use it see the information
    - make sure the information is correct and up to date and we still need to keep it
    - destroy the information when we no longer need it

Keeping information

We will try to keep all our information on a computer or hard drive.

If we need to keep information on paper we will keep it in a locked filing cabinet. We will shred the paper when we do not need the information anymore.

Handling of Data relating to criminal convictions

Information provided about an individual's criminal convictions, including any information released in disclosures, is used fairly, and is stored and handled appropriately and in accordance with the provisions of the Data Protection Act 1998.

Data held on file about an individual's criminal convictions will be held only for as long as is required for employment purposes and will not be disclosed to any unauthorised person.

We always go through the proper DBS channels to establish whether an individual has a criminal record. We will not require job applicants or existing employees to use their subject access rights under data protection provisions to provide criminal record details unless this is required by law.

The relevant DBS disclosure information including level, number, outcome and date will be kept on employees HR

personnel files until such time that it is replaced by a new disclosure.

How we keep information on computers

We use laptops, smart phones and tablets to make, store and look at information.

- All equipment is password protected.
- We only keep information on equipment until it can be uploaded to the cloud.
- All equipment has up to date antivirus and firewalls; these will automatically update.
- Laptops are maintained regularly.
- When a laptop needs to be replaced we will always destroy the hard drive.

We store information in the cloud. We use:

- Dropbox for some work files and images
- Office 365 for contact information and email communication

Our Dropbox folders are secure online. They are owned by one person; only people who need to access them are given permission.

Our information is backed up on an Office 365 system. This is kept secure.

Passwords

Any file that contains information that needs to be safe is protected by its own password. This means that all information that needs to be kept safe is behind at least one password.

When new equipment is being set up or new file or folder is being made to hold information that needs to be kept safe it must be password protected.

Passwords must be:

- changed regularly
- at least eight digits
- have letters and numbers and use capitals

Destroying information

When we no longer need to keep information it is destroyed.

- Paper copies are shredded
- Electronic equipment is wiped before disposal using cleaner
- All hard drives are destroyed before disposal
- Computer files are not just deleted to recycle bin; the bin must be emptied.

We will regularly check the information we have and that it is kept safe.

We will check this policy every year to make sure it is still the best way to look after information.

What we will do if we think something has gone wrong

Before May 25th 2018, organisations which held and used personal data had to report major data breaches to the ICO.

The new law means that organisations must report all personal data breaches to the organisation's Data Protection Lead Officer. All Wales People First's Data Protection Lead Officer is the Business and Finance Manager.

All Wales People First's Business and Finance Manager will decide if the breach is a notifiable one, and if so, he or she will notify the ICO within 72 hours.

If the personal data breach is likely to put individuals at risk, those individuals must be told about the breach straight away.

All Wales People First Staff and volunteers will follow the organisation's Data Protection Policy, and any personal

data breaches will be reported to the Business and Finance Manager.

The Business and Finance Manager is responsible for letting the ICO know within 72 hours.

Who may be responsible for data breaches?

Data protection Law after May 25th 2018 means that individual people who use and process personal data for work are responsible to follow what the law says.

This means that it is not just organisations which can get in to trouble with the law if they do not follow the rules. Staff and volunteers who do not follow the law can be prosecuted too.