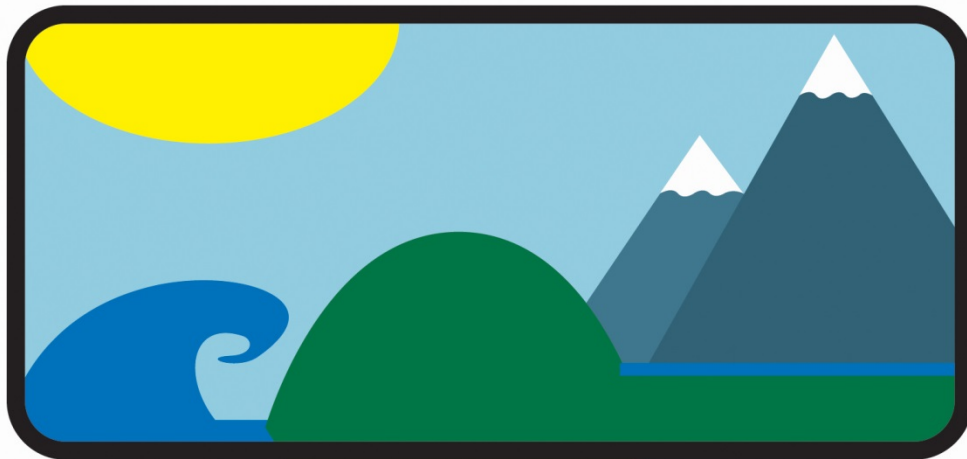


2021

Data Protection Policy

PARTNERIAETH AWYR-AGORED

Profiad • Mwynhau • Llwyddo



Experience • Enjoy • Achieve

OUTDOOR PARTNERSHIP

Tracey Evans

Chief Executive Officer

March 2021

1. BACKGROUND

The Outdoor Partnership was formed in 2004 to promote a vision of an active, healthy and inclusive Wales, where outdoor recreation provides a common platform for participation, fun, achievement and employment, which binds local communities, creates a sustainable use and understanding of the environment of Wales.

Our mission is to improve opportunities for more local people in North West Wales to achieve their potential through outdoor activities.

2. INTRODUCTION

The purpose of this policy is to:

- Complying with the law
- Following good practice
- Protecting clients, staff and other individuals
- Protecting the organisation

Data Protection Act 1998

The Outdoor Partnership will comply with the Data Protection Act which states that anyone who processes personal information must comply with eight basic principles. These being that personal information are:

- Fairly and legally processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer that is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

It also provides individuals the right to find out what personal information is being held electronically, and in most cases, paper records too.

Data Protection Statement

The Outdoor Partnership is committed to guaranteeing the privacy of all persons associated with it and is committed to processing all personal information using the framework provided by the Data Protection Act 1998.

3. PEOPLE, RISKS AND RESPONSIBILITIES

This policy applies to all the staff team at the Outdoor Partnership and all volunteers associated with the organisation. It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include names of individuals, postal addresses, email addresses, telephone numbers plus any other information relating to individuals.

This policy helps to protect the Outdoor Partnership from very real data security risks, including;

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gain access to sensitive data.

Everyone who works for or with the Outdoor Partnership has some responsibility for ensuring data is collected, stored and handled appropriately. All the staff team that handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However the Board of Directors is ultimately responsible for ensuring the company meets its legal obligations. The Chief Executive Officer is responsible for:

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Review all data protection procedures and related policies.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from the staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the Outdoor Partnership holds about them.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

4. SECURITY

Appropriate technical and organisational measures shall be taken against

unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

All Association computers have a log in system and our Contact Database is password protected, which allow only authorised staff to access personal data. Passwords on all computers are changed frequently. All personal and financial data is kept in a locked filing cabinet and can only be accessed by the Chief Executive officer. When staff members are using the laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.

5. DATA STORAGE AND USAGE

Storage

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access accidental deletion and malicious hacking attempts:

- Data must be protected by strong passwords that are changed regularly.
- Data stored on removable media must be stored away securely.
- Data should only be stored on designated drives and servers and only uploaded to the company's approved cloud computing services.
- Data should be backed up frequently.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use:

- When working with personal data, employees should ensure the screens of their

computers are always locked when left unattended.

- Personal data should not be shared informally, in particular via email.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

The Outdoor Partnership will manage sensitive data including

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Membership of a trade union
- Physical or mental health conditions
- Sexual life
- Commission or (alleged commission) of any offense
- Court appearances

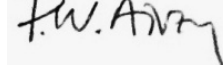
This policy will be reviewed by the Board of Directors on an annual basis.

Last reviewed: March 2021

Signed: 

Name: Tracey Evans
Company Secretary

Date: 25th March 2021

Signed: 

Name: Paul Airey
Chairperson

Date: 25th March 2021