

PACE

Data Privacy Policy

Introduction

PACE is committed to ensuring the personal information we collect, handle and store, as part of our day to day work, is done so in line with the Data Protection Act at all times. When asking for or handling personal information we will ensure that:

- Personal data is processed fairly and lawfully.
- Data is processed only for the purpose(s) for which it was collected.
- Data is adequate, relevant and not excessive.
- Data is accurate and kept up to date.
- Data is not kept longer than necessary.
- Data is kept secure against unauthorised access and loss or damage.

PACE gathers and uses certain information about individuals, including:

- PACE staff.
- PACE volunteers.
- PACE supporters.
- Schools we visit.
- Club members.

This policy describes how personal data will be collected, handled and stored in order to meet the company's data protection standards and ensure legal compliance. Furthermore, we are committed to:

- Complying with both the law and good practice.
- Respecting individuals' rights.
- Being open and honest with individuals whose data is held.
- Acting confidently and consistently.
- Notifying the Information Commissioner voluntarily, even when not required.

Purpose of the policy

The policy applies to:

- Complying with the law.
- Following good practice.
- Protecting individuals who have connection with the organisation in whatever capacity.
- Protecting the organisation.

It applies to all the data that the company holds in relation to identifiable individuals, and can include:

- Names of individuals.

- Postal address.
- Email addresses.
- Telephone numbers.
- Records of our contact such as emails, hand written notes, electronic documents including notes from meetings and training materials.

Data Protection Law

The Data Protection Act 1988 and the Privacy and Electronic Communication Regulations 2003 have been updated in May 2018 and strengthen individual rights and control over the personal information that organisations hold.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The legal framework is underpinned by 8 principles and they say that personal data must:

- Be processed fairly and lawfully.
- Be obtained only for specific, lawful purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Not be held for any longer than necessary.
- Processed in accordance with the rights of data subjects.
- Be protected in appropriate ways.
- Not be transferred outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of protection

Data Protection Risks

This policy helps to protect PACE from some very real data security risks, including:

- **Breaches of confidentiality:** such as information being given out inappropriately.
- **Failing to offer choice:** such as giving individuals the freedom to choose how the company uses data relating to them.
- **Reputational damage:** such as if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or on behalf of PACE are responsible for ensuring data that is collected, stored and handled is done so appropriately and in line with this policy and data protection principles. With this in mind the following general principles are adopted:

- Data is only used in relation to the work that is undertaken.

- Data is not shared informally and without specific consent.
- Data is kept secure by taking sensible precautions as outlined below.
- Strong passwords are used where required and are never shared unless relating to specific documents that are personal to the client.
- Data is regularly reviewed and updated if it is found to be out of date. If no longer required, it is deleted and disposed of securely.

Data collected

The personal information collected will, in the majority of cases, relate to our staff, volunteers and supporters. In such circumstances the data we collect includes:

- Name.
- Contact details: postal address, phone number and email.
- Records of contact: emails, hand written notes, electronic documents such as contracts.

With regards to the children we work with, little data collection is required. This might include names or parental consent forms.

Data storage

The following principles are followed in relation to storage of personal data:

- Where data is stored on paper, it is kept in a secure place where unauthorised people cannot see it. This includes:
 - Storing files in a specific cabinet.
 - Not left out where unauthorised people can see it.
 - Securing and disposing of information when no longer required.
- Where data is stored electronically, it is protected from unauthorised access, accidental deletion and malicious hacking attempts. This includes:
 - Using strong passwords.
 - Using an encrypted removable disc for work ongoing and for backing up documentation. This is then kept securely.
 - Using appropriate encrypted software for storing personal data.
 - Encrypting folders and documents stored data directly to laptops or other mobile devices.
 - Ensuring laptops are appropriately protected.

Data Accuracy

We are committed to take reasonable steps to ensure that the personal data stored is accurate and kept up to date. In order to do this the company will:

- Ensure data is kept in as few as places as necessary.
- Take every opportunity to ensure the data stored is updated.
- Ensure data stored is updated when any inaccuracies are discovered.

Data access requests

Anyone whose personal data is held by PACE are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

This information will be provided free of charge and access requests should be made by email to pace@cwgsy.net

Marketing permissions and information sharing.

PACE will not use your personal information for marketing purposes unless we have your explicit permissions to do so.

Any personal information kept by the company will not be shared with anyone unless specific consent has been gained to do so.

Once given, consent can be withdrawn, but not retrospectively. There may be occasions where the company has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn. This will be discussed with clients as part of the work carried out.

Policy Information

- Policy prepared by: Lisa Griffin, Lee Garland and Janet Fox
- Policy operational from: 17/10/2018
- Policy review date: 01/01/2020