

DRAFT

**DATA PROTECTION & PRIVACY POLICY**

This policy was adopted on ……………………………………………………………………………..

Review date ……………………………………………………………………………………………………

SPUD is currently exempt from registering with the ICO as it is a Charitable Incorporated Organisation (CIO).

Even though SPUD is exempt from registering with the ICO we understand that we are required to comply with all other obligations under the Data Protection Act 1998 as listed below.

1. **WHO IS RESPONSIBLE FOR THE INFORMATION?**

SPUD is responsible for information and also owns the website and it is maintained by ………….We collect website usage information through using cookies. Our website uses cookies to distinguish our users from other users of our website. This helps us to provide our users with a good experience when browsing our website and also allows us to improve our site.

1. **WHAT INFORMATION DO WE COLLECT?**

Spud is responsible for the collection and proper management of any personal information customers, sub-contractors, agents, volunteers and relevant others submit. We will keep personal details secure and use the information provided consistently with applicable privacy and data protection laws and the terms of this Policy.

1. **HOW DO WE USE THIS INFORMATION?**

The information provided may be used in a number of ways, for example:

**3.1** to enable us to keep accurate records of how many individuals, organisations and businesses have shown an interest in SPUD through website/email/social media

**3.2** how many individuals, organisations, businesses have received services, or engaged in person or on-line as individuals or through a business or not-for-profit organisation

**3.3** to understand the geographical areas in which SPUD has had a presence

**3.4** to provide the information, products and services requested and honour any contract

**3.5** for statistical purposes when we evaluate our range and impact of services

**3.6** to personalise repeat visits to our website

**3.7** to inform of other products and services that may be of interest (see section 5 below)

**3.8** to manage customer service queries

1. We will ensure personal information is only used for “fair and lawful” purposes consistent with the individual’s reasonable expectations about what may happen to their details; “Fair and lawful” purposes include where the use of the information:
	1. is necessary to fulfil a legitimate business activity which does not harm the individual concerned – for example where necessary to provide services to the individual;
	2. is necessary to comply with a specific legal responsibility – for example, to notify the tax authorities; or
	3. has been specifically authorised by the individual – for example where they ask for their details to be passed to another person
2. If we engage a third party organisation to process personal information on our behalf (for example using external providers to provide payroll services)

**5.1** we will carry out a security risk assessment to ensure we are confident the third party can keep it safe.

**5.2** We will enter into an appropriate contract with the third party before sharing personal information with them. To keep personal information safe and secure;

**5.3** We will ensure personal information is held within a secure IT system;

**5.4** Ensure any personal information held on laptops, mobile devices and removable data (e.g. USB sticks/ discs) are held in encrypted format;

**5.5** Limit access to personal information held within our organisation to those who will need to access it in order to perform their role;

**5.6** Ensure all personal information is disposed of in a secure manner once it is no longer needed.

**6.** We will not leave personal data insecure in any way, whether it is physical files or information held electronically

**7**. We will not hold personal information about people when it is unnecessary

**8.** We will try to use anonymised personal data where this is possible (e.g. for statistical analysis)

**9.** We will not send personal data outside the European Economic Area without taking action to ensure this can be justified under the DPA.

**10**. We will not use personal information for a different purpose than that for which it was originally obtained unless it is fair to do so in the circumstances.

 **11.** We will take care to ensure personal information is kept accurate and up to date.

 **12.** We will allow individuals the right to access a copy of personal information held about them if they ask for it.

**13.** We will allow individuals the right to opt out from any direct marketing activity we may want to undertake.

**14.** We will be particularly careful when handling sensitive personal data concerning;

**14.1** race or ethnic origin, sexual orientation, political opinion, religious belief, trade union membership, mental/physical health

**We are committed to reviewing our policy and good practice annually.**

This policy was last reviewed on:

…………………………………………………………………………(date)

 Signed: …………………………………………………………….