PWCIC – Project: WILD C.I.C.

General Data Protection Regulations Policy

Contents

1. Data Protection Statement

1.1. PWCIC is committed to a policy of protecting the rights and privacy of individuals, participants, volunteers, staff and others in accordance with The General Data Protection Regulations (GDPR) 2018 and The Data Protection Act 2018. The policy applies to all participants and staff involved with PWCIC. Any breach of GDPR 2018, The Data Protection Act 2018 or The PWCIC General Data Protection Regulations Policy is considered to be an offence and, in that event, disciplinary procedures apply.

1.2. As a matter of good practice, other organisations and individuals working with PWCIC, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff/directors who deal with external organisations will take responsibility for ensuring that such organisations abide by this policy.

2. References

2.1. Data Protection Act (2018) [Link]

2.2. General Data Protection Regulation (GDPR) 2018 [Link]

3. Definitions

3.1. GDPR - General Data Protection Regulations

3.2. DPA - Data Protection Act (2018)

3.3. DPO - Data Protection Officer

3.4. ICO - Information Commissioner's Office

3.5. Use of “us” and “we” refers to responsible individuals within PWCIC

4. Responsibilities

4.1. The appointed Chair is responsible for implementation of this policy. It is their responsibility to ensure that all directors, staff and other team members that could come into contact with sensitive data are suitably trained and have read and understood this policy and the principles underpinning GDPR.

4.2. It is the responsibility of all relevant team members within PWCIC to comply with this policy and handle any personal data they deal with in accordance with the data protection principles. It is important for all staff to take appropriate advice from the appointed Chair when they are unsure about how best to comply.

4.3. Under GDPR (2018) the organisation as currently operating is not required to have a DPO. This will be reviewed regularly as clarified later in the document (8.3.).

4.4. We have determined based on guidelines provided by the ICO that we are currently exempt from paying the data protection fee to register with the ICO. This will be reviewed regularly as clarified later in the document (8.3.).

5. Data Handling

5.1. In accordance with the regulations of GDPR 2018, personal data handled by PWCIC will be:

5.1.1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

5.1.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

5.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.1.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5.1.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

5.1.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2. Legal Requirements

5.2.1. Data is protected by GDPR, brought into effect by the European Union in March 2018. It is also protected by the updated Data Protection Act 2018. Their purpose is to

protect the rights and privacy of individuals and to ensure that personal data is not processed without individual's knowledge and done so with their consent.

5.2.2. This requires us to state the fact that we hold personal data and to acknowledge the right of "subject access" to this data – participants and staff have the right to copies of their own data.

5.3. Purpose of data held by PWCIC

Data may be held and used by PWCIC for the following the purposes:

5.3.1. Staff Administration

5.3.2. Funding and Fundraising

5.3.3. Realising the Objectives of the Organisation

5.3.4. Accounts and Records

5.3.5. Advertising, Marketing and Public Relations

5.3.6. Information and Databank Administration

5.3.7. Journalism and Media

5.3.8. Participants

5.3.9. Research

5.3.10. Volunteers

6. Data Protection Principles

6.1. In terms of GDPR and the DPA, we are the 'data controller', and as such determine the purpose for which, and the manner in which, any personal data are, or are to be, processed. We must ensure that we have:

6.1.1. **Fairly and lawfully processed personal data**

We will always put our logo on all paperwork, stating our intentions on processing the data and state if, and to whom, we intend to give the personal data. We will also provide an indication of the duration the data will be kept.

6.1.2. **Processed for limited purpose**

We will not use data for a purpose other than those agreed by data subjects (participants, staff and others). If the data held by us is requested by external organisations for any reason, this will only be passed if data subjects (participants, staff and others) agree. Also, external organisations must state the purpose of processing and agree not to copy the data for further use.

6.1.3. **Adequate, relevant and not excessive**

PWCIC will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed.

6.1.4. **Accurate and up-to-date**

We will provide data subjects (participants, staff and others) with a copy of their data once a year for information and updating where relevant. All amendments will be made immediately and data no longer required will be deleted or destroyed. It is the responsibility of individuals and organisations to ensure the data held by us are accurate and up-to-date. Completion of an appropriate form (provided by us) will be taken as an indication that the data contained is accurate. Individuals should notify us of any changes, to enable personnel records to be updated accordingly. It is the responsibility of PWCIC to act upon notification of changes to data, amending them where relevant.

6.1.5. **Not kept longer than necessary**

We discourage the retention of data for longer than it is required. All personal data will be deleted or destroyed by us after one year if participation/involvement in the organisation has elapsed.

6.1.6. **Processed in accordance with the individual's rights**

All individuals that PWCIC hold data on have the right to:

- Be informed upon the request of all the information held about them within 40 days.
- Prevent the processing of their data for the purpose of direct marketing.
- Compensation if they can show that they have been caused damage by any contravention of this policy.
- The removal and correction of any inaccurate data about them.

6.1.7. **Secure**

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 Organisation computers have a log in system and our Contact Database is password protected, which allow only authorised staff to access personal data.
- Contact Database passwords are changed frequently.
- All paper and physical copies of personal and financial data is kept in a locked filing cabinet and can only be accessed by directors and senior members of staff.
- 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.

6.1.8. **Not transferred to countries outside the European Economic Area, unless the country has adequate protection for the individual.**

Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual. PWCIC takes particular care to be aware of this when publishing information on the Internet, which can be accessed from anywhere in the world. This is because transfer includes placing data on a web site that can be accessed from outside the European Economic Area.

7. Data Requests

7.1. Data requests that are submitted to PWCIC must be made in writing and submitted to the PWCIC general email address shown at the end of this document.

7.2. PWCIC will aim to respond within 5 working days.

8. Review of this Policy

8.1. PWCIC will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives and as part of our self-evaluation arrangements in line with any feedback from customers/clients, regulatory authorities or external agencies, or changes in our practices, if deemed necessary, by the board of Directors.

8.2. We will review the policy as standard on an annual basis at board meetings.

8.3. Responsibilities points 4.3. and 4.4. will be reviewed before commencement of any new project or contract.

9. Arrangements for Data Security Breach

9.1. Reporting

9.1.1. Confirmed or suspected breaches should be reported within 1 hour to the appointed Chair, who in turn must notify all Directors in writing (electronic methods permitted) within 2 hours of being notified. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data or information is involved.

9.1.2. Once a data breach has been reported, an initial assessment will be made to establish the severity of the breach and who the lead responsible officer should be. All data security breaches will be centrally logged to ensure appropriate oversight of the types and frequency of confirmed incidents for management and reporting purposes.

9.2. Assessing the Risk

9.2.1. Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged, but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences, the risks are very different from those posed by for example; the theft of a customer's confidential information, or data which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, the risks which may be associated with the breach must be assessed. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

9.2.2. The following questions should be helpful in making this assessment:

- What type of data or information is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature, while other data types are sensitive because of what might happen if it is misused (e.g. bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates. If it has been damaged, then this potentially poses a different type and level of risk
- Regardless of what has happened to the data/Information, what could it tell a third party about the individual(s) to whom it relates? Sensitive data could mean very little to an opportunistic laptop thief, while the loss of apparently trivial snippets of

information could help a determined fraudster build up a detailed picture of other people

- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data, but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, or suppliers will to some extent determine the level of risk posed by the breach and therefore our actions in attempting to mitigate it
- What harm can come to those individuals? Are there risks to their physical safety, reputation, financial situation, or a combination of these along with other aspects of their personal life?
- Are there wider consequences to consider, such as a loss of public confidence in an important service we provide?
- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help us prevent their fraudulent use.

9.3. Data Classification

9.3.1. Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved. Therefore, it is important that PWCIC can quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

9.3.2. All reported incidents will need to include the appropriate data classification in order for an accurate assessment of risk to be conducted.

9.3.3. Classification: **Public Data**

Information intended for public use, or information which can be made public without any negative impact for PWCIC.

9.3.4. Classification: **Internal Data**

Information regarding the day-to-day business and operations of PWCIC. Primarily for staff use, though some information may be useful to third parties who work with the PWCIC.

9.3.5. Classification: **Confidential Data**

Information of a more sensitive nature of the business operations of PWCIC, possibly representing its basic intellectual capital and/or knowledge. Access should be limited to only those people that need to know as part of their role(s) within the PWCIC.

9.3.6. Classification: **Highly Confidential Data**

Information that if released through improper actions will cause significant damage to PWCIC's business activities or reputation or would lead to a breach of the General Data Protection Regulation. Access to this information should be highly and carefully restricted.

9.4. Responsibility of Lead Responsible Officer (LRO)

9.4.1. LRO responsible for assessing the risk and preparing a preliminary report of the breach.

9.4.2. Within 24hrs of being notified of the breach the LRO must;

- Contact any individuals whose data may be compromised
- Contact independent supporting organisation(s) for advice on how to proceed: *Selby District AVS*.

- Contact the ICO in order to register if necessary and complete an ICO Data Protection Breach Notification Form.
- Proceed as advised by the ICO.

10. Version Details

Policy Effective from Date: 13th October 2019
Policy Review Date: October 2020
Signed by Chair (Nicholas Atherton):

Version:……2.0
Last Updated:……13/10/2019
Last Reviewed by Board:……13/10/2019