**Data Protection Audit for [name of charity]**

General Data Protection Regulation is a new EU law that will come into effect on 25/5/18 to replace the current Data Protection Act (1998). It represents a significant change in data protection compliance for all organisations. Essentially, it introduces additional requirements for how organisations process personal data and aims to give back control to EU citizens over their data. The Information’s Commissioner’s Office have provided [12 step plan](https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf) as a reliable basis for commencing work towards compliancy (i.e being transparent about data you hold, updating privacy notices, planning how to handle request for data, identifying a lawful basis for processing personal data, consent, having procedures in place to report a data breach)

The Charity needs to demonstrate compliance with the new data protection laws by having proper control and management of personal data, defined as “*data which relates to a living individual who can be identified from that data or other information which is in the possession of the data controller”.* In order to complete a data audit*,* employees and trustees need to create a current inventory of the personal data they process and map the processing of personal data they each collect. This will help us to identify the compliance measures we already have in place so we can establish what we must do to ensure that all we do is GDPR compliant.

**Name of staff member/trustee:**

**Role at The Charity**:

**Date you completed this audit:**

1. **Why do you keep or process personal data?**

Some examples of why personal data is used at The Charity may include:

* Grant application administration
* Champion newsletters
* Direct marketing activities
* Legal obligations i.e tax, work permits

|  |
| --- |
| 1. List why you use or process any personal data |
|  |
|  |
|  |
|  |
|  |
|  |

1. **Whose personal data do you use or process?** List all the different categories of persons about whom you keep or process personal data.

**S**ome examples of categories of persons may include:

* Staff (current and former)
* Champions
* Support club members
* Immediate beneficiaries
* Donors
* Third party supporters
* Trustees

|  |  |  |
| --- | --- | --- |
| Whose personal data is it | What’s your reason for processing it or keeping it | Do you share this personal data with anyone? |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **What personal data do you use, keep or process?** List all different types of personal data you use/keep, and identify the source of the data (individual, third party, DBS, government departments), where it is located (email, filing cabinet, desk computer, computer drives, phone), why you retain this personal data.

Some examples of types of personal datainclude:

* Personal details i.e name address contact number, DOB, ethnicity
* Financial details i.e bank account, NI, tax reference
* Information relating to health
* Employment data i.e when someone begins employment at The Charity
* Photographs
* Passport and National ID card details

|  |  |  |  |
| --- | --- | --- | --- |
| Type of personal data | Source of personal data | Location of personal data | Why do you retain this personal data |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **When is personal data processed?** – Processing data includes obtaining, disclosing and deletion of personal data. List all the times when you process personal data. State if you know:

* When do you obtain the personal data?
* Who would you disclose the data to and why?
* How long do you keep the data for?

Retention periods may be determined by: A statutory requirement – clearly identify which section of law or regulation sets out the retention period and the minimum and/or maximum period OR A business/professional practice

|  |  |  |  |
| --- | --- | --- | --- |
| When do you process or update personal data? | Who else has access to the data? (i.e disclosures to third parties) | Retention period? What would determine the period? | How is the data protected from loss/unlawful use? |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Where do you process the personal data?** – Examples of where processing occurs include:

* Manually/written – what and where
* Electronic – password protected or shared
* Database systems
* Working at home
* Cloud services

|  |  |  |  |
| --- | --- | --- | --- |
| Type of personal data (State reason for processing) | Manual or written record? (Yes/No and Location) | Electronic record? (Yes/No – Location) | System used (if any) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Data Collection Methods**

The Charity utilises some of the following data collection methods. Please specify which of these data collection methods you use. Add any data collection methods that are not listed below.

|  |  |
| --- | --- |
| Data Collection Method | Do you use the data collection method? (Yes/No and Explain) |
| Employee application forms |  |
| Grant application forms |  |
| Email exchange |  |
| Database CRM |  |
| Website contact form |  |
| ACC training modules |  |
| Online surveys |  |
| Written correspondence |  |
| Org Sheets |  |