



**Maindee Unlimited** - UK Charity No: 1160272

## **Data protection and GDPR policy and guidelines**

### **1. Policy Statement**

Maindee Unlimited is working to transform Maindee into a sustainable community with a strong local identity, strong local economy, and a reputation as an attractive, safe, culturally vibrant and cohesive place to live, relax in and work. We are committed to reflecting this vision of safety in the way we store and process personal data.

### **2. Data Protection and GDPR Policy & Guidelines**

Organisations and people who we hold information on are referred to in this policy as data subjects.

The Data Protection Act 2018 requires us to have a data controller who is responsible to the Trustees for this policy and should notify non-exempt data processing to the Information Commissioner. John Hallam, Programme Manager, is the current data controller.

The General Data Protection Regulation (GDPR) is an EU regulation that harmonises data protection policies and guidelines across EU member states.

- We hold three types of information which are covered by this policy
  - publicly available information
  - personal information, typically in the form of mailing lists and containing information about individuals such as names, addresses, job titles
  - sensitive personal information – in general this kind of information is only held about employees. There are, however, instances where sensitive information is held about other people. For example information about dietary requirements at a conference might allow a person's religion or health status to be deduced.
- We will not hold information about individuals without their knowledge and consent.
- It is a legal requirement that people know what we are doing with their information and who it will be shared with.
- We will only hold information for specific purposes. We will inform data subjects what those purposes are. We will also inform them if those purposes change.
- We will seek to maintain accurate information by creating ways in which data subjects can update the information held.

- Information about data subjects will not be disclosed to other organisations or to individuals who are not members of our organisation, staff or trustees except in circumstances where this is a legal requirement, where there is explicit or implied consent or where information is publicly available elsewhere.
- Data subjects have the option not to receive marketing mailings from us or other organisations.
- Data subjects will be entitled to have access to information held about them by us and for what purpose within 40 days or submitting a request.
- Subject to any rules of the organisation awarding the funding, information will not be retained once no longer required for its stated purpose, we will not keep more than a project requires or surplus information 'just in case'. We will establish retention periods and a process to delete personal information when no longer required. Sensitive data, such as data about unspent convictions received by the organisation as part of DBS checks, will not be retained for more than three months,
- At the beginning of any new project or collection of any new type of data, the member of staff managing it will consult the data controller about any data protection implications.
- There may be situations where we work in partnership with other organisations on projects which require data sharing. We will clarify which organisation is to provide data control and will ensure that the data controller deals correctly with any data which we have collected.

### **Data Security**

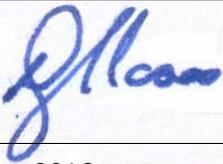
- We have procedures for ensuring the security of all electronic personal data. Paper records containing confidential personnel data are disposed of in a secure way. Project documents and staff records are all kept in a locked filing cabinet, IT equipment containing personal information is kept in a locked room or cupboard when not in use.
- All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep our information secure from would-be thieves. There is no point protecting the personal information we hold with a password if that password is easy to guess.
- We will make sure that personal data temporarily held on portable devices – such as sticks, PCs and laptops – are deleted in a timely way. Weekly housekeeping is additionally advised.

### **Our Commitment**

- We have a set of procedures covering all areas of our work which we follow to ensure that we achieve the aims set out above.
- We will take regular back-ups of computer data files which will be stored away from the source location in a safe and secure place.
- Staff and volunteers will be given training on this policy and procedures. They will be told how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.
- We will carry out an annual review of our data protection policy and procedures.

## Data Protection Principles

1. Personal data should be processed fairly and lawfully
2. Personal data should be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required
4. Data should be accurate and kept up-to-date
5. Data should not be kept for longer than is necessary for purpose
6. Data processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organizational measures should be taken unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EU unless that country or territory ensures an adequate level of data protection.

Name DAVID MOSES	Name JOHN HALLAM
Office CHAIRPERSON	Office PROGRAMME MANAGER
Signature 	Signature 
Date: October 2016	Date: October 2016

Initial Policy: October 2016

Reviewed: March 2019