**Okehampton Community**

**Recreation Association**

**Data Protection Policy**

Adopted: 07.01.16

Reviewed:

**Introduction**

OCRA needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards, and to comply with the law.

This policy is to ensure that OCRA:

* Complies with data protection law and follow good practice
* Protects the rights of staff, customers and partners
* Is open about how it stores and processes individuals’ data
* Protects itself from the risks of data breach

**Data Protection Law**

The Data Protection Act 1998 describes how organisations, including OCRA, must collect, handle and store personal information. 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 data Protection Act is underpinned by eight important principles, these say that personal data must:

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

**Policy Scope**

This policy applies to all Trustees, staff and volunteers of OCRA. Also any contractors, suppliers and other people working for and on behalf of OCRA.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

* Names of individuals
* Postal addresses
* Email addresses
* Telephone numbers
* Club membership details

**Data Protection Risks**

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

* **Breaches of confidentiality.** For instance, information being given out inappropriately.
* **Failing to offer choice.** All individuals should be free to choose how the company uses data relating to them.
* **Reputational damage.** The company could suffer if personal information was made public.

**Responsibilities**

Everyone who works for or with OCRA has some responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

* The Trustees are responsible for ensuring that OCRA meets its legal obligations.
* The Office Manager will:
1. Keep the Trustees updated about data protection responsibilities, risks and issues.
2. Review all data protection procedures and related policies in line with an agreed schedule.
3. Arrange data protection and advice for the people covered by this policy if required.
4. Handle data protection questions from staff and anyone else covered by this policy.
5. Deal with requests from individuals to see the data that OCRA holds about them (also known as ‘subject access requests’).
6. Check and approve and contracts or agreements with third parties that may handle the company’s sensitive data.
7. Ensure that suitable checks are made, by qualified contractors, to ensure all systems, services and equipment used for storing data meet acceptable security standards. Also ensure that regular checks are made to security hardware and software.

**General Staff Guidelines**

* The only people able to access data covered by this policy should be those who need it for their work.
* Data should not be shared informally. When access to confidential information is required employees can request it from their line manager.
* OCRA will provide training to all employees to help them understand their responsibilities when handling data.
* Employees should keep all data secure by taking sensible precautions and following the guidelines below.
* Strong passwords must be used and should never be shared.
* Personal data should not be disclosed to unauthorized people, either within or without the company.
* Data should be regularly reviewed and updated if found to be out of date. If no longer required it should be deleted and disposed of.
* Employees should request help from their line manager or office manager if they are unsure about any aspect of data protection.

**Data Storage**

This is to describe how and where data should be safely stored.

* When data is stored on paper it should be kept in a secure place where unauthorized people cannot see it.
* If stored electronically any printed material should be:
1. Kept in a locked drawer or filing cabinet when not needed.
2. Not left where unauthorized people could see them, like on a printer.
3. Data printouts should be shredded and disposed of securely when no longer required.
* Electronically stored data must be protected from unauthorized access, accidental deletion and malicious hacking attempts.
* Data should be protected by strong passwords that are changed on a regular basis and never shared between employees.
* If data is stored on a removable device (like a disc or memory stick) these should be kept locked away when not being used.
* Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
* Servers containing personal data should be sited in a secure location.
* Data should be backed up frequently, and should be tested regularly.
* Data should never be saved directly to a laptop or other mobile device, in particular to a private ones.
* All servers and computers containing data should be protected by approved security software and a firewall.

**Data Use**

Personal data is of no value to OCRA unless the business can make use of it. However it is when it is accessed and used that it can be at the greatest risk of loss, corruption or theft.

* When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
* Personal data should not be shared informally. In particular it should never be sent by email as this form of communication is not secure.
* Data must be encrypted before being transferred electronically.
* Personal data must never be transferred outside of the European Economic Area.
* Employees should not save copies of personal data to their own computers or other mobile device.

**Data Accuracy**

The law requires OCRA to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the data is accurate, the greater the effort OCRA should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept accurate and up to date as possible.

* Data will be held in as few places as necessary. Staff should not create any unnecessary data sets.
* Staff should take every opportunity to ensure data is updated, for instance by confirming a customer’s details when they call.
* OCRA will make it easy for data subjects to update the information OCRA holds about them.
* Data should be updated as inaccuracies are discovered. For example if a customer can no longer be contacted on their stored information it should be removed from the database.

**Subject Access Requests**

All individuals who are the subject of personal data held by OCRA 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.

If an individual contacts the company requesting this information, this is called a subject access request.

Requests made from individuals can be made via email or post, addressed to the Office Manager at finance@ocrasport.org.uk or Pavilion in the Park, Okehampton EX20 1GE.

Individuals may be charged up to £10 per subject access request, depending on the level of work required. The aim will be to provide the relevant data within 14 days. The identity of anyone making the request will be verified before handing over any information.

**Disclosing Data For Other Reasons**

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances OCRA will disclose requested data, however, the office manager will ensure the request is legitimate, seeking assistance from the Trustees and legal advisers where necessary.

**Providing Information**

OCRA aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights.

To these ends the company has a privacy statement setting out how data relating to individuals is used by the company, which is available on request.