Curdridge Reading Room and Recreation Ground Charity

Trustee, Employee and Volunteer obligations under the Data Protection Act

The Chairperson of the Curdridge Reading Room and Recreation Ground Charity assumes overall responsibility for ensuring the Charity complies with its data protection obligations. *The terms of trustee, employee, member and volunteer are all interchangeable within this document. It is recognised that some policy areas are not applicable to all groups. The term and use of 'associate' is included for ease and covers all four groups.*

On commencement with the Charity, associates will be made aware of the information that will be held about them and how this will be used and disclosed. This information may include personal data such as address, contact details, date of birth or age, salary, bank details, pension and sickness records. An employee's consent to hold this information will be sought by the inclusion of an appropriate clause in their employment contract.

Associates are responsible for ensuring that all personal data provided by them to the Charity is accurate and updated when appropriate.

Associates will be informed of their right to make a Subject Access Request and will be referred to the access request policy.

Associates will be reminded annually of their obligations under the Data Protection Act. Associates handling data will be referred to the Charity's guidelines on the collection, storage, use and destruction of records in line with the data and privacy policy. Associates will be made aware that they could be criminally liable if they knowingly or recklessly disclose personal information in breach of the policy and, as a minimum, that serious breaches of the policy will be a disciplinary matter (applicable to employees).

By signing this document, you are confirming that you have read and understood what is contained within it and that you will comply with the requirements that apply to you in your capacity as an associate of the Charity.

Signed:

Printed Name:

Date: To be reviewed:

Curdridge Reading Room and Recreation Ground Charity

Procedure for dealing with Subject Access Requests (Data Protection Act)

On receipt of a Subject Access enquiry by any Trustee, employee or volunteer of the Charity, the person asking for their information will be asked to put their request in writing to the Chairperson or a designated Trustee of the Charity.

The person requesting the information will be asked to include:

- Details of the specific information they require and any relevant dates;
- The reason for the request, if deemed appropriate.

The Associate of the Charity will reply within 40 days, starting from the date the written request is received.

The individual requesting the information will be:

- Told whether any personal data is being processed;
- Given a description of the personal data, the reasons it is being processed and, whether it will be shared with any other organisations or people;
- Given a copy of the information consisting of the data itself as well as details of the source of the data (where this is available).
- An explanation of any technical or complicated terms if required.

The Associate of the Charity may withhold information if it contains information that relates to another person. Unless the other person gives their permission, or it is reasonable in all the circumstances to provide the information without permission, the Charity is entitled to withhold this information.

By signing this document, you are confirming that you have read and understood what is contained within it and that you will comply with the requirements that apply to you in your capacity as an associate of the Charity.

Signed:

Printed Name:

Dated: To be reviewed:

Curdridge Reading Room and Recreation Ground Charity
Recommendations for the Retention of Information and Documents

Personal data shall not be kept any longer than is necessary for the purpose that it has been collected for. The Curdridge Reading Room and Recreation Ground Charity will follow retention guidelines as laid down by the Information Commissioner's Office.

The retention guidelines are as follows:

Statutory Retention Periods

Record	Statutory retention period	Statutory authority
accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).
accounting records	3 years for private companies, 6 years for public limited companies	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
income tax and NI returns, income tax records and correspondence with HMRC	not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676)
medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
medical records under the Control of Asbestos at Work Regulations • medical records containing details of employees exposed to asbestos • medical examination certificates	• 40 years from the date of the last entry • 4 years from the date of issue	The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)
medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years.	The Ionising Radiations Regulations 1999 years of age, but in any (SI 1999/3232)
records of tests and examinations of control systems	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations

and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)		1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
Records relating to children	Until the child reaches 21	Limitation Act 1980
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894)
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970

Non-Statutory Retention Periods

Actuarial valuation reports	permanently
Application forms and interview notes (for unsuccessful candidates)	At least 1 year
Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently
Inland Revenue approvals	Permanently
Money purchase details	6 years after transfer or value taken
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Pensioners' records	12 years after benefit ceases
Personnel files and training records (including disciplinary records and working time records)	6 ears after employment ceases
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Senior executives' records (that is, those in a senior management team or their equivalents)	Permanently for historical purposes
Time cards	2 years after audit

Trade union agreements	10 years after ceasing to be effective
Trust deeds and rules	permanently
Trustees; minute books	Permanently
Works council minutes	permanently

Volunteer Personal Information

It is good practice to review the personal information held on volunteers regularly. The Curdridge Reading Room and Recreation Ground Charity is committed to reviewing this information annually and any information no longer required will not continue to be stored.

By signing this document, you are confirming that you have read and understood what is contained within it and that you will comply with the requirements that apply to you in your capacity as an associate of the Charity.

Signed:

Printed Name:

Dated: To be reviewed:

Curdridge Reading Room and Recreation Ground Charity

Information Security and Security Breach Notification Policy

This document is concerned with information held by the Reading Rooms Charity and used by the members of the Charity in their official capacities i.e. as Trustees, Members, Employees, or, where appropriate, Volunteers (Charity Associates). It relates both to computer-based and paper-based information and defines the responsibilities of individuals with respect to the use of that information.

All Charity Associates are directly responsible for the information they handle. Failure to comply with this policy, and other associated policies, may result in disciplinary action. Associates of the Charity must:

- Be aware of this policy and comply with it,
- Understand which information they have a right to have access to through the course of their duties performed on behalf of the Charity,
- Know the information for which they are owners,
- Know the information systems and computer hardware for which they are responsible.

For the purpose of this document, information security is characterised as being concerned with guaranteeing *availability* i.e. ensuring that authorised users always have access to information when they need it; *integrity* i.e. safeguarding its accuracy and completeness; *confidentiality* i.e. ensuring that sensitive information is accessible only to those authorised to use it; and authenticity. It also addresses methods of disposal of information that is no longer required.

Types of information retained by the Charity

- Hirers - Personal information of hirers of the facilities including hiring history, contact details, bank account details, information generated by enquiries and any directly related correspondence
- Trustees – information required by the Charity Commission, contact details, details of specific roles and / or responsibilities;
- Donations – anonymous donations – any information is to be destroyed once the donation has been received and confirmed
- Online payments – financial transaction details will be recorded in the bank account and by surname/amount in cashbook spreadsheet. Any published accounts will hold cumulative amounts. Electronic payments for tickets and events will be encouraged through PayPal.
- Volunteers - contact details, skill sets, availability, any directly related correspondence and historical volunteering information.
- Employees - personal details, contact information, employment records and any other records relating to an individual employed by the Charity will be held in accordance with Data Protection.

- Events - details of projects or events organised by the Charity, details of suppliers or trades assisting with the event / project, attendance information, financial information.
- Hires – bank details obtained for sole use of returning deposits will be deleted once deposit is returned.
- Invoices – electronic and paper invoices received may contain bank account details, contact details, VAT numbers
- Members – personal details and contact information will be held after a written application has been received and will be removed on resignation of the individual. A member who is a representative of an organisation may be proposed by that Organisation but personal confirmation will also be sought.

Access to Information and Classification

Associates of the Charity will have access to information according to its classification. Information will be classified into one of the following categories:

- Public or Open categories,
- Confidential,
- Strictly Confidential,
- Current
- Up to date and accurate
- Historic i.e. held for good reason as a record.

Historic information may be archived, that is, retained but removed as a prime information source and possibly stored in a pared – down form.

Information must be destroyed when there is no valid reason for retention. Disposal must be considered when the information is first acquired as highlighted in the principles of the data protection policy.

Public information may be viewed by anyone.

Information defined as ‘open’ refers to that information where access is available to all members of the Charity who have a legitimate right to access that information and have the right to access any such paper- based or computer-based systems accordingly.

Information defined as ‘confidential’ will only be accessible to specified associates of the Charity with appropriate authorisation from the Trustees.

‘Strictly confidential’ information will be controlled and restricted to a small number of named individuals.

Incident Handling

Any associate of the Charity must report any information security incident to the appropriate Trustee.

Incidents will be investigated by the Chairperson plus any other Trustee/s as agreed by the Trustee Committee. Where appropriate, the outcome of the investigation will be fed back to the Trustee Committee upon which, the Trustee Committee will determine whether and what course of action to be taken i.e. revisiting and reviewing information security safe-guards, instigating disciplinary action etc.

Implementation

Procedures will be put in place in order to ensure effective information access and security control. The objective of these procedures is to ensure that:

- Information users are appropriately identified and have access to information for which they have a legitimate need,
- Computer systems are appropriately managed and controlled in line with the requirements of this policy,
- Information assets are identified and protected (An information asset is any group of information that can be managed as a 'single unit' so that it can be understood, shared, protected and exploited effectively such as a database of contacts, files / records associated with a specific project or financial data about the Charity),
- There is clear assignment of responsibilities.

Procedures will include:

- User registration procedures and password usage for access to email and any other shared computing facilities
- Control of access to Charity computer networks, network system security, intrusion detection, prevention and remedial action
- Systems security procedures including administration, monitoring and logging, virus protection and, where appropriate, encryption
- Backup of computer systems
- Inventory of information assets, including equipment, software and data
- Information access control for different classifications of information & regular review of user access rights
- Disaster recovery and business continuity in the face of an incident
- Physical security of computer rooms, networks, personal computers, computer maintenance and disposal

Storage of computer-based information

Email – data held within the Charity's email system is secure and backed up on a quarterly basis

Shared data files – information that originates on a PC using documents, spreadsheets or databases should be stored on a drive that can be accessed by all those requiring access to it.

Users should store Charity Information Assets on this shared drive and not on the local hard disk drive of their machine. Access to this drive is secure as it requires a

password of the owner to access the file space. By default, no other user has access to the data. Other users may be granted access to individual folders (or even files) within this shared drive; they should only have access to the data to which the owner has granted access and need to give their username and password when accessing the shared information.

Use of desktop PC's

Computer-based Information Assets held on PCs or other systems at the Reading Rooms are not normally secure against theft, damage due to fire, flood, vandalism or other incidents. The information held on these systems must be secured to ensure that anyone who gains unauthorised access to the physical machine cannot obtain access to the information stored on its hard disk i.e. password protected files. Information held on these systems must also be backed up on a regular basis and the back-ups must be regularly tested (to ensure that the data can be restored).

Charity Information Assets should not be stored on desktop PC's which are located on non-Charity premises, unless authorised to do so by the Trustees.

Use of Laptop Storage

Charity Computer-based Information Assets held on laptops must be password protected and should also be stored on the 'shared drive'. The user must establish a working regime that copies changed data onto the shared drive on a regular basis so as not to put any information 'at risk'.

Users of Laptop systems need to be vigilant and take appropriate steps to ensure the physical security of the laptop at all times. Access to all laptop systems must be controlled by the use of proper usernames and passwords.

Storage of paper-based information

Charity paper-based information must be stored in a secure location and access only given to those information users who have a legitimate need.

Disposal of Information

Computer-based and paper-based information will be reviewed regularly, and any information stored that is no longer required will be disposed of in a secure manner i.e. paper-based information will be shredded and computer-based information will be deleted from any drives where it is held. Once computer-based information is deleted the system will need to be backed up as soon as possible to ensure that only up-to-date information is held.

It is understood that on occasion it is appropriate for historical information to be retained possibly for future analysis or comparison of figures. Such information should be stored in a pared-down form and any personal data removed wherever possible.

Security Breach Notification

Any suspected or confirmed information security breaches must be reported immediately to the Chairperson or any other Trustee of the charity. A breach is defined as unauthorised access of Charity information. The Chairperson and any other trustee as agreed by the Trustee Committee will investigate all reports of security breaches.

A security breach may arise from:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire or flood;
- Hacking attack;
- Information being obtained by deceiving the organisation who holds it ('Blagging attack)'

Upon notification of a suspected information security breach, and within 72 hours of notification, the Chairperson or any other nominated trustee will report the breach to the appropriate authority (if applicable) and to the affected individuals. Depending upon the type of breach and the information involved the Police, appropriate banks or the media may be advised.

Should an Associate of the Charity become aware of an information breach, it is their responsibility to bring it to the attention of the Chairperson or a nominated Trustee as soon as possible.

This policy will be reviewed and amended regularly to ensure that it remains relevant and in line with the appropriate data protection regulations.

By signing this document, you are confirming that you have read and understood what is contained within it and that you will comply with the requirements that apply to you in your capacity as an associate of the Charity.

Signed:

Printed Name:

Dated: To be reviewed: