Data Protection Policy

Data Protection Officer: Joe Walker, Director

Trustee with responsibility for data protection: Abi Kingston

1. Overview:

The Round Chapel Old School Rooms (RCOSR)/Clapton Park URC is committed to processing data in accordance with its responsibilities under the General Data Protection Regulations (GDPR). This policy recognises that SNSC has a duty to protect the personal information of staff, volunteers, donors and contacts it is responsible for.

The charity understands that it is the custodian of personal information. The charity recognises the importance of handling personal data securely and appropriately. Personal data is understood through the definition in Article 5 of the General Data Protection Regulations (GDPR) 2018 act[1].

2. Review

The charity will undertake to review this policy every 12 months. The policy will also be reviewed when necessary – for example, in the event of legislative or organisational change.

3. Purpose and Objective:

RCOSR is fully committed to compliance with the requirements of the Data Protection Act 2018 and all other data protection legislation currently in force. The Regulation applies to anyone processing personal data and sets out principles which should be followed and gives rights to those whose data is being processed.

To this end, RCOSR endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency');

[1] The Information Commissioner's Office define personal data' as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

- processed no further than the legitimate purposes for which that data was collected ('purpose limitation');
- limited to what is necessary in relation to the purpose ('data minimisation');
- accurate and kept up to date ('accuracy');
- kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation');
- processed in a manner that ensures security of that personal data ('integrity and confidentiality');
- processed by a controller who can demonstrate compliance with the principles ('accountability').

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, RCOSR will:

- observe fully the conditions regarding having a lawful basis to process personal information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements;
- ensure the information held is accurate and up to date;
- ensure that the information is held for no longer than is necessary;
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 2018 (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information);
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection.

4. Employees' Personal Information

Throughout employment and for as long as is necessary after the termination of employment, RCOSR will need to process data about employees. The kind of data that SNSC will process includes:

- any references obtained during recruitment;
- details of terms of employment;
- payroll details;
- tax and national insurance information;
- details of job duties;
- details of health and sickness absence records;

- details of holiday records;
- information about performance;
- details of any disciplinary and grievance investigations and proceedings;
- training records;
- contact names and addresses;
- correspondence with the Charity and other information that you have given the Charity.

RCOSR believes that those records used are consistent with the employment relationship between the Charity and employee and with the data protection principles. The data RCOSR holds will be for management and administrative use only but RCOSR may, from time to time, need to disclose some data it holds about an employee or volunteer to relevant third parties, for example where legally obliged to do so by HM Revenue & Customs, where requested to do so by the employee for the purpose of giving a reference or in relation to maintenance support, and/or the hosting of data in relation to the provision of insurance.

In some cases RCOSR may hold sensitive data, which is defined by the legislation as special categories of personal data, about employees. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet RCOSR's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, employees will be asked to give express consent for this information to be processed, unless the Charity has a specific legal requirement to process such data.

5. Access to Data

Employees may, within a period of one month of a written request, inspect and/or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections should such records be faulty. The Charity is entitled to change the above provisions at any time at its discretion.

6. Data Security

Trustees, employees or volunteers are responsible for ensuring that any personal data that they hold and process as part of your job role is stored securely.

They must ensure that personal information is not disclosed orally, in writing, via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

They should note that unauthorised disclosure may result in action under the Disciplinary Procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and, where possible, it should be locked away out of sight, for example in the boot of a car. You should avoid travelling with

hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight, for example in the boot of a car.

7. IT and Communications

RCOSR reserves the right to access and monitor the use of all Charity owned digital devices, including monitoring internet, telephone and email use unless the IT equipment is the property of the employee.

All of our work takes places outside an office environment. Staff and volunteers all use mobile devices such as laptops, tablets, smartphones and USB sticks The term that most organisations adopt when allowing staff to purchase their own equipment and use it for work purposes is BYOD, or Bring Your Own Device.

If the purchase price of the equipment is paid or reimbursed by RCOSR then the device is owned by RCOSR. If it has not been reimbursed then the equipment belongs to the individual staff member.

Employees must take the appropriate steps to guard against unauthorised access to, alteration, accidental loss, disclosure or destruction of data.

Under no circumstances should you divulge your password to anyone else nor should you gain access or attempt to gain access to information stored electronically which is beyond the scope of your authorised access level.

You are responsible for any activity which occurs within your accounts.

Personal use of computer and telephone systems is not permitted. Personal telephone calls may be accepted in exceptional circumstances with the agreement of your Manager.

Storage of personal files, images, software, or Apps on the Charity network or devices is not permitted.

You must not use the Charity internet connections or devices to access content that is illegal, pornographic, or supports hate and/or discrimination.

You must not send communications via any Charity or personal device that could be deemed to be offensive.

The use of any device to photograph or film fellow employees, customers, clients, visitors, or any member of the public without their consent may breach an individual's right to privacy and could in certain circumstances constitute harassment.

This policy should be read in conjunction with all other Charity policies and rules, including policies on equality and positive work environment.

As with other written communication, email is a legally binding method of communication. Other forms of communication via the internet may also be legally binding. All forms of communication whether verbal or written represent RCOSR and should therefore meet the standard and style expected of all communications.

Because of potential virus infection and consequent damage to the business, you must not download or load any software into any computer via any source, including memory sticks, flash drives, pen drives, any portable memory devices, or mobile phones without the prior approval of management. Approval will only be given after virus checking.

Downloading free software or Apps is permitted where there is a valid business reason and the software or App is considered to be from a reputable source.

You must not make pirate copies of Charity owned software for use by other persons either inside or outside the Charity. This not only breaks Charity rules, it is an illegal practice.

Company devices may contain tracking facilities. The Charity may use these as follows:

- for the prevention and detection of theft of devices;
- to protect the health and safety of our employees;
- as a method of checking the accuracy of Charity records, such as timesheets.

You must not tamper with any tracking facility or device. Tampering with tracking may lead to action under the Disciplinary Procedure up to and including summary dismissal.

8. Social Media

RCOSR recognises that some employees will have personal social media accounts. Such accounts must only be used to express personal views, and care should be exercised in all cases where you are identifiable as someone employed by RCOSR.

RCOSR requires employees using social media sites to refrain from making any comments or engage in discussions which could adversely affect the Charity or the Charity's reputation, or our supporters of donors. It is also prohibited to breach discrimination legislation, harass or bully an employee, or damage working relationships between fellow employees.

You must not share any confidential or sensitive RCOSR information on social networks.

You are personally responsible for all content posted on your accounts. All passwords must remain secure, and you must never leave accounts open whilst you are away from your device or computer.

You are reminded that regardless of the social network used, or privacy settings activated, everything posted on the internet has the potential to become public and widespread. All social media posts should therefore be carefully considered to ensure they fit with the image you and the Charity want to share online.

You may also be required to remove content created or shared by you if the Charity consider such posts to be a breach of this policy.

All RCOSR rules and policies apply in respect of social media posts. This policy therefore should be read in conjunction with all other policies, in particular your attention is drawn to the RCOSR policies on equality and positive work environment.

9. Notifying Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a data controller or data processor;

- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

10. Investigation and Notification

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by the Director or Chair of Trustees.

We will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

We will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

11. Record of Breaches

SNSC records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under the Data Protection Act 2018. It records the facts relating to the breach, its effects and the remedial action taken.