Data protection & confidentiality policy

1. Introduction

1.1 Ripon City of Sanctuary (RCoS) regards the lawful and correct processing of personal and special category data (sensitive personal data) as an integral part of its functions and vital for maintaining confidence between ourselves and service-users, volunteers, supporters and other stakeholders about whom we process personal information/data.

1.2 RCoS recognises that the EU General Data Protection Regulation (GDPR), which became effective from 25 May 2018, provides a comprehensive framework for confidentiality but that it does not cover all circumstances and therefore a confidentiality policy is also required (see section 14)

1.3 The GDPR gives every living person (or their authorised representative) the right to apply for access to the personal data which organisations hold about them, irrespective of when and how they were compiled, ie electronic and manual records held in a structured file, subject to certain exemptions. This is called a 'data subject access request' (see section 8 of this policy).

2. Aims and objectives

2.1 This data protection policy explains how RCoS will meet its legal obligations concerning confidentiality and information security standards. The requirements within the policy are primarily based upon the GDPR, which is the key piece of legislation covering information security and confidentiality of personal information. The objectives of this policy are to: -

- establish a clear and agreed understanding of what confidentiality means within RCoS
- set out the way in which personal information/data should be protected and transferred within RCoS
- clearly state RCoS's legal obligations to comply with the GDPR
- encourage uniformity in practice and ensure that service-users, volunteers, supporters and other stakeholders know what they can expect from RCoS.

3. Definitions

RCoS will protect personal information/data falling into 2 categories as defined by the GDPR:

3.1 **Personal information/data** relates to a living individual who can be identified from the information (or from that information and any other information in the possession of RCoS). This includes:

- factual information
- expressions of opinion about the individual
- indication of the intentions of the RCoS data controller
- any other person in relation to the individual concerned
- any data where an individual can't be identified immediately, but additional subsequent information may permit their identification.

3.2 **Sensitive personal information/data** attracts additional protection and is considered by the Information Commissioner's Office (ICO) to be any data that could identify a person. Example of this would include personal data consisting of information such as:

- the racial or ethnic origin of the data subject
- their political opinions
- their religious beliefs or other beliefs of a similar nature

- their physical or mental health or condition
- their sexual orientation or activity
- details of their bank account, national insurance number, and/or any ID details such as biometric residence permit, UNHCR card, CV, passport, driving licence, etc
- their membership (or otherwise) of a trade union.

Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside of the EU's legislative competence).

3.3 '**Personal data' may also include 'sensitive personal data' and must be processed lawfully, fairly and in a transparent manner** in relation to individuals.
The GDPR also requires you to have a "condition" (legal basis) for processing the personal data:

a) at least one of the conditions in article 6 of the GDPR must be met ('Lawful basis for processing')
b) in the case of sensitive personal data, at least one of the conditions in article 9 of the GDPR must also be met (see Appendix I, 'The conditions of processing', for further detailed information).

For the purposes of clarity, the term "personal data", used throughout this document, refers to either personal information/data and/or sensitive personal information/data, as appropriate.

3.4 **A record** can be in computerised and/or manual form. It may include such documentation as:

- hand-written notes
- letters to and from RCoS
- electronic records, including email, messaging apps, and storage on hard-drives, portable devices or Cloud storage
- print-outs
- photographs
- videos and tape recordings.

All data relating to an individual may need to be made available in response to a 'subject access request' (see section 8 below). Back-up data also falls under the GDPR; however, a search within backup data should only be conducted if specifically requested by the data subject.

3.5 **Data subject** means an individual who is the subject of personal data. This could include service-users (service-users) volunteers, supporters and representatives of third-party organisations (such as a local authority, Refugee Council or other CoS group).

3.6 **Data controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed.

3.7 **Data processor** (in relation to personal data) means any person who processes that data on behalf of the data controller – other than a volunteer colleague of the data controller.

3.8 **Third party** (in relation to personal data) means any person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor.

3.9 **Processing** means recording or holding information or data or carrying out any operations on that information or data; including organising, altering or adapting it; disclosing the information or aligning, combining, blocking or erasing it.

3.10 **Service-user** indicates a user of the services of RCoS. This is likely to mean refugees and asylum-seekers.

3.11 **Volunteer** indicates anyone authorised by RCoS to deliver services to service-users on its behalf, and can include members of the management committee.

4 Policy statement

4.1 The main focus of this policy is to provide guidance about the protection, sharing and disclosure of service-user and volunteer information. **The duty to maintain confidentiality and adhere to data protection legislation applies to all committee members and volunteers of RCoS.**

4.2 The GDPR requires that most organisations register with the ICO and describe the categories of information they hold about people, and what they do with it. Since it is deemed to be a charity, RCoS is not required to register; it must, however, observe the legislation fully and must observe the rules around reporting breaches.

4.3 There are 6 data protection principles which lie at the heart of the GDPR (article 5) and give the GDPR its strength and purpose. To this end, RCoS fully endorses and abides by the principles of data protection. Specifically, **the 6 principles** require that data is:

1 processed lawfully, fairly and in a transparent manner in relation to individuals

2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay

5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

6 processed in a manner which ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against **accidental loss, destruction or damage**, using appropriate technical or organisational measures.

4.4 **Personal data** is defined in section 3 of this policy.

4.5 Compliance with these principles is the very essence of both (a) compliance with the law and (b) good practice. The ICO has powers to interpret the principles and, subject to the interpretation provisions of the GDPR, the Information Tribunal and the courts, to give advice about how to comply with the law, and enforce its provisions where this is necessary to achieve compliance. Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller.

4.6 Therefore, RCoS will, through appropriate management, and strict application of criteria and controls:

4.6.1 ensure that there is a **lawful** ground for using the personal data

4.6.2 ensure that the use of the data is **fair** and will meet one of the **specified conditions** (see Appendix I)

4.6.3 only use sensitive personal data if it is **absolutely necessary** for RCoS to use it (see Section 3 – paragraph 3.2)

4.6.4 only use sensitive personal data where RCoS has obtained the individual's **express consent**, unless an exception applies

4.6.5 **explain to individuals**, at the time their personal data is collected, how that information will be used

4.6.6 only obtain and use personal data for those purposes which are **known to the individual**

4.6.7 personal data should only be used for the **purpose** it was given; if RCoS needs to use the data for **other purposes**, further consent may be needed

4.6.8 only keep personal data that is really **relevant** to RCoS

4.6.9 where required, keep personal data **accurate** and **up to date**

4.6.10 only keep personal data for **as long as is really necessary** and in any case no longer than 5 years for service-users (based on the standard period of 'leave to remain' authorised by the Home Office) and, for volunteers, up to 2 years after the end of the period of volunteering

4.6.11 always adhere to our **subject access request procedure** and be **receptive** to any queries, requests or complaints made by individuals in connection with their personal data

4.6.12 always allow individuals to **opt out** of receiving marketing information. RCoS must always **suppress** the details of individuals who have opted out of receiving marketing information

4.6.13 will always **give an option** to "opt out" when **consent** is needed to share personal data unless there is a statutory purpose for doing so

4.6.14 take appropriate technical and organisational security measures to **safeguard** personal data.

In addition, RCoS will ensure that:

4.6.15 there is a volunteer with specific responsibility for data protection within RCoS (the 'data protection lead')

4.6.16 everyone managing and handling personal data understands that they are responsible for following good data protection practice

4.6.17 everyone managing and handling personal data is **appropriately trained** to do so, and that appropriate advice is available. Training and refresher training is a mandatory requirement for all committee members and volunteers **every 2 years.**

4.6.18 everyone managing and handling personal data is appropriately supervised

4.6.19 enquiries about handling personal data are promptly and courteously dealt with

4.6.20 methods of handling personal data are clearly described (See section 6 - operational practice)

4.6.21 an annual internal audit is to be made of the way personal data is managed by the data owners listed in section 9.2

4.6.22 methods of handling personal data are regularly assessed and evaluated

4.6.23 performance with handling personal data is regularly assessed and evaluated.

5. Scope of the policy

The scope of this policy extends to:

- service-user records
- volunteer records
- financial records.

6. Operational practice

RCoS is a dispersed organisation with no offices or computer equipment of its own. Instead, management committee members and volunteers rely on their personal equipment and their homes

for processing and storing personal information. This means that it is especially important that RCoS management committee members and volunteers understand their responsibilities, and should:

6.1.1 stop and consider whether they should be processing personal data before they do so

6.1.2 make sure that they have verified that the person they are passing data on to is who they say they are and that they are authorised to receive it

6.1.3 not discuss information about service-users, committee members, volunteers, supporters or other stakeholders with unauthorised colleagues, family or friends, or service-users (see also Section 14, 'confidentiality')

6.1.4 not access RCoS business records containing personal data other than for a specific business purpose. This may also be an offence under GDPR and RCoS may be prosecuted by the ICO.

6.1.5 avoid providing any specific detail about individuals that might lead to their identification when using information for reports or monitoring purposes unless they have given written permission for it to be used

6.1.6 not express unsubstantiated personal opinions in file notes, e-mails or other means of communication; individuals may have a right to see the information and may exercise that right

6.1.7 give careful consideration to the use of e-mail distribution lists and use the blind carbon copy (BCC) option especially when sending out e-mails to large numbers of recipients

6.1.8 always remember to consult the chairperson, and if necessary the data protection lead, before starting any projects involving the processing of personal data

6.1.9 avoid storing and printing documents (whether created personally or viewing documents created by others) on personal hard drives; instead, create, comment on, and edit documents in Google Drive and set up links to make those files accessible in a secure way (for example, setting up a password-protected Word file containing those links)

6.1.10 always consider data security, and the risks associated with losing personal data, before downloading or printing any personal data

6.1.11 password-protect their computer and never share that password or write it down; doing so could result in the unauthorised accessing of personal data and, therefore, a serious security breach

6.1.12 encrypt any mobile phone on which personal information may be sent received or stored, by email, SMS or other messaging service, file storage or access to cloud storage (biometrics, swipe pattern, PIN, etc); volunteers will be asked to sign to this effect, and a record will be kept by the data protection lead, reviewed every 2 years (since mobile phones are changed regularly)

6.1.13 always secure their screen when leaving their computer by pressing the Windows key and 'L' simultaneously (even if it's only for a few minutes) and switch off at the end of the day and when absent from where the computer is located, for example out for the day or on holiday

6.1.14 never read or work on any RCoS data in a public place, including use of paper, mobile phones and laptops

6.1.15 take care not to leave documents containing personal data on printers, photocopiers or scanners (even at home where they could be seen by friends or family members). Fax machines should not be used to transmit personal data as the ICO considers it out-dated and insecure

6.1.16 ensure that personal data cannot be seen or accessed by unauthorised individuals either at or away from home or other place or work, and store it securely in a lockable cabinet. If sensitive data is taken out of a building, it needs to be in a locked bag. When travelling by car, papers must always be transported in the boot of the car. Papers must not be left in the car overnight; when at home they should be stored in a locked bag or secured cabinet.

6.1.17 remember to dispose of confidential waste and paper copies containing personal data in special bins or by shredding.

6.1.18 ensure personal data extracted for RCoS use is stored on encrypted memory sticks or other suitable encrypted storage. Data uploaded to any third-party online storage facility must be treated with the same level of security, and permission must be sought in advance of any upload – see Section 7 below.

6.1.19 extract data only with approval from the RCoS chairperson; the control of the data whilst extracted is the joint responsibility of the "data extractor" and the chairperson

6.1.20 never add a name to the RCoS marketing mailing list, or ask for a name to be added, without first having secured permission in writing to do so from that supporter, and ensuring that they understand how their contact information will be used. This evidence must be passed to the data protection lead, who will store it appropriately.

7. Transfer of data to a third party

7.1 Before personal data is transferred, a non-disclosure agreement (NDA) or data processing agreement should be in place between RCoS and the third party. Either agreement should clearly state the third party's obligation to treat the data in accordance with the provisions of the contract, the reasons for the transfer, the time period, what it is required for, how it will be processed and what actions will be taken to delete data when no longer needed.

7.2 NDAs and data processing agreements are managed by the data protection lead and committee members and volunteers should ensure that they have checked with the data protection lead that the **appropriate agreement is in place** before organising a transfer of personal data. If you are in doubt which document should be used, please consult the data protection lead.

7.3 Note that NDAs and data processing agreements are only valid for the data transfer within the EEA and anything else is not permissible (unless special arrangements are made). Where data is to be transferred outside of the EEA then EU Model Contract Clauses must be in place.

7.4 Once an agreement is in place, data that is to be transferred through email, upload sites, USB sticks, CD-ROMs or similar formats should be secured. Only encrypted USB sticks should be used. All data files should also be password-protected and preferably zipped and encrypted. Where relevant, no such device should be sent through the open post – a secure courier service must always be used. The recipient should be clearly stated (See section 10).

7.5 If data is sent via a courier the intended recipient must be advised when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received, and liaising with the courier service if there is any delay in the receipt of the data.

7.6 Data must not be transferred beyond RCoS other than to an authorised recipient, such as a partner or contractor. If sent via the internet, identifying the individual should be avoided (for example, by using the individual's first-name initial); alternatively, all personally identifiable data must be either password-protected and/or encrypted.

8. Rights of access by individuals

8.1 Under the GDPR, any living person, who is the subject of personal data held and processed by RCoS, has a right to apply for access to that information. This is known as a **data subject access request.**

8.2 An individual does not have the right to access information recorded about someone else, unless they are an authorised representative.

8.3 It is important that the Data Processor ensures that third-party information is removed from the record prior to release to the applicant unless the third party has given their consent to the release of the information.

8.4 What is a subject access request?

8.4.1 The GDPR ensures transparency of processing personal data by obliging data controllers to explain to individuals how their data will be used, and by providing the right of data subjects to access that information.

8.4.1 A data subject may make a formal request to any organisation to have a copy of all data in which that person may be identified. There is a need for transparency of processing to ensure that individuals can identify those organisations which have access to and process their data. This enables them to understand how their personal information is to be used and to exercise their rights over the processing of that information.

8.4.1 The importance of the right of subject access in Data Protection law cannot be overestimated; it is often only by exercising the right to see their information that individuals can determine whether other breaches of legislation have occurred. Data subjects are often interested in documentation which may be about them but which they have not seen.

8.4.1 Because of the importance of the subject access rights, complaints about an organisation's failure to comply with a request for subject access are taken very seriously by the Information Commissioner. Such complaints are dealt with as a matter of priority and may often lead to a full-scale investigation into an organisation's procedures and practices.

9. Roles and responsibility

RCoS has a duty to ensure that the requirements of the GDPR are upheld.

9.1 Data protection lead

The RCoS management committee appoints one of its members to the post of data protection lead (this individual is named at the end of this policy). This individual's responsibilities include:

- Ensuring compliance with legislation principles (including all points in section 4.6 of this policy, especially with regard to informing service-users), including maintaining records
- In consultation with the management committee, reviewing and adapting this policy **annually** in order to help volunteers understand their responsibilities in the context of RCoS
- Providing training to volunteers in relation to compliance with legislative requirements, keeping records of that training and ensuring it is refreshed **every 2 years**
- Providing ongoing guidance and advice to volunteers in relation to compliance with legislative requirements
- Ensuring notification of processing of personal data to the information commissioner is up to date
- Reporting on any breaches of data protection legislation.

In the data protection lead's absence, advice can be gained from http://www.ico.gov.uk/

9.2 Data owners

Committee members and volunteers are responsible for information they hold manually and electronically and for adhering to, and contributing to the development of, procedures in relation to data protection within RCoS. As data owners, their responsibilities within parameters of this guidance include:

- being generally aware of the significance and demands of the relevant legislation
- being familiar with this data protection policy and carrying out their responsibilities towards service-users, volunteers, the committee, supporters, and individuals employed by third-party organisations
- Informing the data protection lead of any changes in the processing of personal data
- Identifying and justifying how sets of data are used
- Identifying all personal data for which they are responsible
- Agreeing who can have access to the data.

9.3 Management committee

9.3.1 The management committee, with the support of the data protection lead, is responsible for ensuring that members and volunteers are aware of their obligations by producing relevant policies and providing training for existing and new individuals

9.3.2 All committee members and volunteers handling personal information about service-users, management committee members, volunteers, supporters or individuals from other organisations are required to complete RCoS' data protection training and read and understand this policy, raising any necessary questions to facilitate that understanding.

9.3.3 Newly recruited volunteers and committee members are required to read this policy and undergo data protection training within the first month of joining RCoS, regardless of any prior knowledge of data protection.

9.3.4 The management committee will ensure that there is a named data protection lead is always in place and that they are aware of their responsibilities.

9.4 All volunteers and contractors

9.4.1 Maintaining confidentiality and adhering to data protection legislation applies to all committee members and volunteers. RCoS will take all necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice and, where appropriate, bound by a common-law duty of confidence.

9.4.2 These responsibilities and common law duties apply equally to all transient volunteers and workers/consultants engaged to carry out work on behalf of RCoS. Further responsibilities include:

- Observing all guidance and codes of conduct in relation to obtaining, using and disclosing personal data
- Obtaining and processing personal information only for specified purposes
- Only accessing personal information that is specifically required to carry out their work
- Recording information correctly in both manual and electronic records
- Ensuring any personal information held is kept secure
- Ensuring that personal data is not disclosed in any form to any unauthorised third party
- Ensuring sensitive personal information is sent securely. (See Section 10)

9.4.3 **Failure to adhere to any guidance in this policy could result in volunteers individually being criminally liable for deliberate unlawful disclosure under the GDPR**. This may result in criminal prosecution and/or disciplinary (including being removed from the management committee or volunteer list).

9.5 **The Information Commissioner's Office (ICO)**

The Information Commissioner's Office is responsible for overseeing compliance, eg investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers. Any failure to comply with GDPR may lead to investigation by the ICO which could result in serious financial or other consequences for the company.

10. Sending personal sensitive information externally

10.1 Service-user data

10.1.1 RCoS regularly processes personal information to assist its service-users and provide services.

10.1.1 The GDPR requires that all organisations have appropriate security in place to protect personal information against unlawful or unauthorised use or disclosure, and accidental loss, destruction or damage.

10.1.1 The following guidance sets out how personal or sensitive information should be processed to ensure data is properly secured. This includes the transferring, storage and disposal of information and information held on our behalf by contractors.

10.1.1 If you have personal information that is currently stored or transferred insecurely, you must secure it immediately.

10.2 Justification

10.2.1 All volunteers have a duty to ensure that information (about service-users, management committee members, volunteers, supporters) and sensitive non-personal information is handled appropriately. Sensitive information should only be made available to people authorised to view it.

10.2.2 The following principles should be followed wherever you communicate sensitive personal information:

- Justify the purpose for sharing the information
- Do not use information that personally identifies individuals unless necessary
- Information should be disclosed on a "need to know" basis
- If unsure then seek guidance on appropriate action from the data protection lead.

10.3 Face to face

Personal information should not be shared in front of others. Volunteers should ensure that they are not disclosing or requesting the disclosure of sensitive information about themselves in front of others, or in a format that could be viewed by others.

10.4 Telephone

Personal information should only be disclosed over the telephone to a third-party where the following procedure has been adhered to:

10.4.1 The identity of the other party has been confirmed by verification. The type of verification will differ by service and the sensitivity of the information being disclosed. For queries by service-users we require their name, address and postcode. For third parties we require consent from the service-user before releasing/confirming that they are a service-user of RCoS.

10.4.1 The reason for requesting the information has been established and is appropriate.

10.4.1 Where appropriate, contact details have been requested and their identity checked by calling the person back via the main switchboard of the organisation that they represent and asking for the person by name (unless already known).

10.4.1 Provide personal information only to the person who requested it.

10.4.1 Do not leave any confidential information on voicemail or answering machines as it may be accessible by others. Please remember that by confirming an individual is a service-user of RCoS you are releasing personal information as defined by the GDPR.

10.4.1 When in conversation, take precautions to ensure that information is not shared inappropriately with others, eg when using mobile phones, travelling on trains, etc.

10.4.1 Sensitive personal information should not be sent via text messaging as it may be accessible by others.

10.5 Email

Email services should be used as follows:

10.5.1 Sensitive information relating to a single individual can be sent via email attachment to the subject of the information if they have requested it to be sent by email or with their agreement and it is encrypted. The exception for this is when the recipient has stated that they want to receive the information without encryption. A record must be kept of this.

Documents containing sensitive personal information cannot be sent to third parties without encryption and should not be contained within the body of an email but attached as an encrypted document (eg password-protected).

10.5.2 Care should be taken when addressing email messages to ensure a correct, current address is used and the email is only copied to those with a legitimate interest.

10.5.3 If information is transmitted and not received by the intended recipient, check that contact details and email address are correct for the receiving party before re-sending.

10.5.4 Consider the impact on individuals of the data being lost or misdirected. Where information is provided in bulk or where the information is of a sensitive nature make an assessment on the protection to be applied. If in doubt, send information in an encrypted attachment to the email.

10.5.5 Avoid putting sensitive personal information about more than one person in an email as this will lead to difficulties in maintaining accurate and relevant individual service-user or volunteers records.

10.5.6 When transferring data be aware of who has permission to view your emails or who might be able to view your recipient's inbox.

10.5.7 Where email and personal data are stored or accessed on any mobile device, such device must be protected with a password/PIN/finger print or other secure login means

10.5.8 Wherever possible, avoid using service-users' full names; where known to the recipient, the initial of the first name only should be used (eg 'M' or 'M's wife'). Avoid using further identifying information, such as their address, within the same communication.

11 Breach of policy

In the event that a volunteer or committee member fails to comply with this policy, the matter may be considered as misconduct and dealt with accordingly.

12 Dealing with a data breach

12.1 If a data breach is suspected, the committee member or volunteer should **immediately**

- Notify the RCoS chairperson
- Notify the data protection lead by filling in the first section of the Information Security Incident Report (Appendix IV)

12.2 Following notification RCoS will take the following actions urgently:-

- Implement a recovery plan, including damage limitation
- Assess the risks associated with the breach
- Inform the appropriate people and organisations that the breach has occurred
- Where required, report the breach to the ICO
- Review our response and update our information security

13 Confidentiality

GDPR legislation deals with information which is written down and organised in a structured way. Beyond that, because of the nature of its work, RCoS is also likely to be made aware of many sensitive, personal and private ('confidential') issues which are not subject to GDPR legislation but which affect service-users, volunteers and supporters. This information may be verbal or in writing, and must still be handled appropriately. It should only be made available to people authorised to know it and where a legitimate case can be made for sharing.

13.1 Basic principles for sharing information

Whenever you share information which could be deemed to be confidential, ask yourself:

- whether sharing this information is **warranted**. Can you make a legitimate case for why it was necessary to share it?
- whether you are sure that the information you are sharing is **true and correct**. If you are not certain, but still feel that it is important to share what you believe, ensure you make this clear to the person with whom you are sharing the information.
- how the **subject might feel** about your sharing it, and (a) how you would justify to the subject *why* you shared the information, and (b) how you would justify your choice of *who* you told
- whether the **person** to whom you share the information to (a) needs to know, and (b) is the right person to share this information with
- whether sharing this information is **fair** both to the subject (are you abusing their trust? Do you have a legal responsibility to share?) *and* to the person with whom you are sharing it (does it put them in a difficult position? Will they feel unnecessarily burdened?)
- whether this information needs to be written down, at which point is becomes subject to (a) GDPR legislation (b) data subject access requests. A careful judgment should be made, taking into account the seriousness of the circumstances, but a general principle is that timely verbal communication with one or more members of the management committee may be the preferred starting point.

Volunteers not discuss information about service-users, committee members, volunteers, supporters or other stakeholders with unauthorised colleagues, family or friends, or service-users

13.2 Legitimate cases for sharing information

- When sharing confidential information between volunteers could benefit RCoS's work on behalf of its service-users; for example, in helping to improve services, share experiences or good practice, seek advice, or provide mutual support.
- When volunteers have concerns about service-users or other volunteers. Example scenarios include:
  - If a client discloses circumstances which may be detrimental to their wellbeing (requiring additional care or support), or which may indicate cases of harm, abuse or neglect
  - If a volunteer has suspicions of service-users or volunteers engaging in illegal activity (benefits fraud, terrorism, money-laundering, smuggling, people-trafficking, etc). Volunteers should be aware that failing to take appropriate action could make them an 'accessory after the fact' and potentially liable to prosecution and punishment as if they were a principal offender.
  - If it is felt, through disclosure or observation, that a volunteer is being taken advantage of by a service-user.

13.3 Responsibilities of the RCoS management committee

The management committee will

- ensure that volunteers are trained in this confidentiality policy.
- refer to and adhere to the RCoS Children Safeguarding Policy and the Adult Safeguarding Policy
- not disclose confidential information beyond the management committee without the approval of its chair (except in an emergency), and when doing so will keep a record detailing all relevant circumstances and how the information was shared.

14 Approval, appointed lead and review date

Date approved: 11 September 2018
Appointed lead: Nicola David
Next review date: September 2019

Appendix I – The conditions of processing

This section explains the conditions that need to be satisfied before you may process personal data.

In brief – what does the GDPR say about the "conditions for processing"?
The first data protection principle requires, among other things, that RCoS must be able to satisfy one or more "conditions for processing" in relation to its processing of personal data. Many (but not all) of these conditions relate to the purpose or purposes for which it intends to use the information.

The conditions for processing take account of the nature of the personal data in question. The conditions that need to be met are more exacting when the information being processed is sensitive personal data, such as information about an individual's race, health, faith or political views.

However, the ICO view is that in determining if there is a legitimate purpose for processing personal data, the best approach is to focus on whether what the organisation intend to do is fair. If it is, then it is likely to be possible to identify a condition for processing that fits that purpose.

Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately. So it makes sense to ensure that what the organisation wants to do with personal data is fair and lawful before worrying about the conditions for processing set out in the Act.

In more detail… What are the conditions for processing?
The conditions for processing are set out in Article 6 and 9 to the GDPR. Unless a relevant exemption applies, at least one of the following conditions must be met whenever personal data is processed:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)

(d) **Vital interests:** the processing is necessary to protect someone's life

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

What is the "legitimate interests" condition?
The GDPR recognises that organisations may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided certain requirements are met.

The first requirement is that RCoS must need to process the information for the purposes of its legitimate interests or for those of a third party to whom it discloses it.

The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. RCoS's legitimate interests do not need to be in harmony with those of the individual for the

condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

What conditions need to be met in respect of sensitive personal data?

At least one of the conditions must be met whenever personal data is processed. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Service-user State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the service-users or to former service-users of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) the processing relates to personal data which are manifestly made public by the data subject;

(f) the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) the processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

When is processing "necessary"?

Many of the conditions for processing depend on the processing being "necessary" for the particular purpose to which the condition relates. This imposes a strict requirement, because the condition will not be met if the

organisation can achieve the purpose by some other reasonable means or if the processing is necessary only because the organisation has decided to operate its business in a particular way.

What is meant by "consent"?
One of the conditions for processing is that the individual has consented to their personal data being collected and used in the manner and for the purposes in question.

The circumstances of each case will need to be examined to decide whether consent has been given. In some cases this will be obvious, but in others the particular circumstances will need to be examined closely to decide whether they amount to an adequate consent.

The GDPR defines an individual's consent as:

> "…any ***freely given*** specific and informed indication of his wishes by which the data subject ***signifies his agreement*** to personal data relating to him being processed".

The fact that an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but consent should not be inferred if an individual does not respond to a communication – for example, from a failure to return a form or respond to an electronic read receipt.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if RCoS intends to continue to hold or use personal data after the relationship with the individual ends, then the initial consent to the processing of personal data should cover this.

Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in the information is collected or used. Withdrawing consent does not affect the validity of anything already done on the understanding that consent had been given.

Whether consent has been given is an issue that should be reviewed as the relationship with an individual develops, or as the individual's circumstances change.

Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

The GDPR distinguishes between:

- The nature of the consent required to satisfy the first condition for processing; and
- The nature of the consent required to satisfy the condition for processing sensitive personal data, which **must be** "explicit".

This suggests that the individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

For these reasons RCoS should not rely exclusively on consent to legitimise its processing. In the Information Commissioner's Office view it is better to concentrate on making sure individuals are treated fairly rather than on obtaining consent in isolation. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing personal data.

For further information you can contact the ICO hotline which gives advice to the public and organisations on data protection/confidentiality or visit http://www.ico.gov.uk/

Appendix II – Data access request form

Please note that whilst it is not obligatory to complete this form but information contained within it would help RCoS to respond to your request in the most efficient manner.
Name:
Address:
Reference number:
Telephone number:
By completing this form you are making a request under the General Data Protection Regulation for information held about you by RCoS that you are eligible to receive.
Required information:
By signing below you indicate that you are the data subject named above. RCoS cannot accept requests from anyone else such as family service-users regarding your personal data. We may need to contact you for further identifying information before with your request. You warrant that you are the data subject and will fully indemnify us for all losses, cost and expenses if you are not. Please return this form to the data protection lead at RCoS at info@ripon.cityofsanctuary.org Please allow 30 days for a reply.
Data subject's signature and date

Appendix III – subject access requests: further information

1.0 What is a valid subject access request?

- It must be in writing, either hard copy or e-mail. Reasonable adjustments should be made if a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing.
- It must request access to their personal information (held either manually or electronically) and not to information relating to other people.
- If a request does not mention the GDPR specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.
- It may be restricted to only limited information (but need not be).
- It must be made by the data subject (or by a person authorised by the data subject). RCoS will take reasonable steps to verify that the person making the subject access request is the data subject.
- It must be complied with within 30 calendar days from the date of receipt

2. Finding and checking the requested information

If an employee receives a subject access request for information, the request should immediately be sent to the data protection lead who within 30 days will go through the following process: -

- Notify each department manager of the request and ask them to search all of the systems for personal data relating to the individual;
- Collate all information and ensure on the requesters personal data is disclosed (redacting any third party data);
- Securely send the response to the verified address of the data subject;
- Retain a copy of the disclosed data.

3. Denial of access

The GDPR includes various exemptions which specify the circumstances in which an organisation can refuse to provide access to personal data.

Access can be refused if RCoS has previously complied with an identical or similar request in relation to the same individual, unless a reasonable interval has elapsed between compliance with one request and the receipt of another.

RCoS can also refuse to provide the data if the effort in doing so would be disproportionate.

There are a number of other instances when RCoS may refuse access.

3.1 Access to all or part of a record will be denied if one or more of these conditions exist:-

a) In the opinion of the relevant professional the information to be disclosed would be likely to cause serious harm to the physical or mental health of the applicant or any other person.

b) If the information forms part of legal advice given to the service-user by an RCoS solicitor or a solicitor acting on behalf of RCoS and is therefore covered by legal professional privilege.

c) The release of data would jeopardise the prevention or detection of crime, or the apprehension or prosecution of offenders;

d) The data is contained in a confidential reference provided by RCoS;

e) The request records RCoS's intention in relation to any negotiations with that person , and the release of the data would prejudice negotiations;

f) The data relates to management forecasting or management planning and its release would prejudice RCoS's business activities;

g) The person has requested access to data which relates to research and the results of the research have not been published in a manner which identifies individuals

3.2 Notification of any refusal to grant access will be given as soon as possible, in writing. RCoS will record the reason for this decision, and will also fully explain the reason to the applicant unless doing so would itself disclose information which would be subject to the exemption.

3.3 Even if RCoS is aware that the applicant has received a copy of the information from another source, it must provide a copy of the information if held.

4 Exemptions

4.1 RCoS has to protect the rights and other legal rights of other individuals when responding to a subject access request. If the release of personal data would reveal information which relates to and identified another person (third party) for example, where a relative has provided certain information, this information will be withheld unless consent from the third party individual is obtained, and it would not be reasonable in the circumstances to release the data without their consent.

4.2 If the release of personal data is likely to cause serious harm to the data subject's physical or mental health or of any other person it may be withheld.

4.3 There is an exemption in the GDPR that allows personal information to be disclosed for the purposes of preventing or detecting fraud and for attempting to secure the apprehension of offenders, but there are limits on what can be released. When a decision is made to release personal data for this purpose, a detailed record of the reason why should be kept.

Appendix IV – data breach incident report

Notes in blue are for guidance and should be read before being over-written by your responses.

Reported by *name (need not be the breaching individual)*

Date of this report *date*

Summary of the event and circumstances	*Where, date, what, who, etc*
Type and amount of personal data	*Title or name of the document/s, and the personal information it contained (eg name? address? health?)*
How was the original breach discovered, and by whom?	*If originally discovered by a third party, how did RCoS discover the breach?*
Actions taken by recipient when they inadvertently received the information	*Did they read, delete, forward it, etc? Did they inform the data subject?*
Actions taken to retrieve information and respond to the breach	*Were they asked to do anything, eg delete the information, and how do we know they did it?*
Policy in place	*Should adherence to the RCOS Data Protection & Confidentiality Policy have prevented this breach? Which sections?*
Procedures/instructions in place	*Should the breaching individual have known how to avoid this breach? What procedures had they been asked to follow re the communication, secure storage, sharing and exchange of information, prior to this incident?*
Details of data protection training provided	*Include information about the last training given to the breaching individual, prior to this incident*
Has a complaint been received from the data subject?	
Details of notification to affected data subject	*Has/have the data subject/s been notified? If not, why not? What advice has been given to the data subject/s?*
Has the ICO been informed?	*Explain reasons why/why not*
Procedure changes to reduce risks of future data loss	*Eg does the policy need to be amended? Does new training need to be given?*
Conclusion	*Eg has this been a minor or serious breach? Is this likely to happen again?*