Confidentiality, Data Protection and Sharing Information Policy

Contents

Purpose and scope	.....	**2**
Definitions	.....	**2 - 4**
Roles and responsibilities	.....	**4**
Multi-agency information sharing principles and protocols	.....	**5**
Formal information sharing protocols	.....	5
Service users' data	.....	**5 - 10**
Confidentiality statement and gaining informed consent to share information	.....	6 – 7
Withdrawal of consent	.....	7
Sharing information with consent	.....	7
Sharing information without consent	.....	7 – 8
Sharing sensitive personal data without consent	.....	8
Sharing non-sensitive personal data without consent	.....	9
Considerations when supporting children and young people	.....	9
Transfer of data to other agencies	.....	10
Trustee, employee and volunteer data	.....	**10**
Subject Access Requests (SARs)	.....	**10 – 14**
Timescale	.....	11
Verifying identity	.....	11
Searching for the relevant information	.....	11
Supplying the requested information	.....	11
Recording SAR handling	.....	11 – 12
Exemptions	.....	12
Special cases	.....	12
Refusing a request	.....	13
Service user case notes	.....	13 – 14
Staff personnel files	.....	14
Further information	.....	14
General issues in respect of confidentiality and the work of CRCC	.....	**14 – 16**
Training	.....	**16**
Breach of policy and confidentiality	.....	**16 – 17**
Complaints	.....	16 – 17
Information to the police and other investigating agencies	.....	**17 – 18**
Third parties	.....	17 - 18

Digital version: [Ctrl] + [Click] on the hyperlinks above (underlined) to take you to the relevant section.

Purpose and scope

Cambridge Rape Crisis Centre (CRCC) is committed to maintaining the highest standards of confidentiality in all of its work in order to ensure the safety and wellbeing of service users, staff and volunteers. During the course of CRCC's work we will collect, store and process personal information about service users, employees and volunteers.

Inappropriate breaches of confidentiality may have life-threatening consequences (amongst others) and will result in disciplinary action.

We recognise it is vital to work with other organisations to fulfil our obligations in respect of the safety and well-being of employees, service users and others. We will at all times endeavour to do this within the confines of legal requirements and best practice.

This policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

CRCC is also committed to safeguarding the rights of service users and workers to access information that is held about them and wherever possible gaining consent to share information about them within the legal and practice parameters set out in this document.

The policy is internal and applies to all staff (including sessional staff), volunteers, and trustees. The confidentiality principles continue to apply after their service or involvement with the charity has ended.

In fulfilling the above aims, CRCC will work within the requirements of the following legislation and practice guidance:

- UK General Data Protection Regulations (UK GDPR)
- The Data Protection Act 2018
- The Human Rights Act 1998
- The Children Act 2004
- The Crime and Disorder Act 1998

Related policies

This policy details how we collect, store and process personal information about service users, employees and volunteers and is used in conjunction with our 'Privacy Policy', which covers how we collect, store and process personal information about supporters and the public.

This policy should also be read in conjunction with our 'Safeguarding Children and Adults at Risk Policy'

Definitions

Workers means CRCC staff members and volunteers collectively.

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

In line with provisions of the Data Protection Act 2018 and the UK General Data Protection Regulations, employees, volunteers and trustees working for Cambridge Rape Crisis Centre will ensure that all personal data is:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate
- Not kept longer than necessary for the purpose
- Processed in line with data subjects' rights
- Secure
- Not transferred to people or organisations situated in countries without adequate protection

Fair and lawful processing

For personal data to be processed lawfully, certain conditions are imposed, chiefly that of obtaining the subject's consent, or where processing is necessary for the legitimate interest of CRCC or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases, explicit consent to the processing of such data will be required.

Accurate data recording

Personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

Data security

CRCC ensures that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes.

CRCC will take steps to ensure security though:

- **Password and Multi-Factor Authentication** - All data is kept confidential using strong passwords and, wherever possible, Multi-Factor Authentication for electronic records. Paper records are securely locked in filing cabinets or drawers. All data must be cleared from desks and locked away each evening or when not in use. Password information should be kept by each individual and not disclosed to any other person inside or outside the organisation.

- **Equipment** – All data users should ensure that individual monitors do not show confidential information to passers-by and that they log off/close their PC when it is left unattended. All data users are responsible for keeping the relevant software, particularly security and anti-virus software, on their CRCC-provided equipment regularly updated.

- **Authorised removal** – Paper records must not be removed from the building, without prior permission from the Director unless it is being used for a case conference or where an individual is required to give evidence in a court of law. Electronic records should, where possible, only be accessed using CRCC-provided equipment (e.g. laptop and work mobile) and must not be duplicated without permission from the Director. If personal equipment has to be used, it is up to the data user to ensure sufficient security is in place on the personal device and that electronic records are never saved on local hard drives.

- **Methods of disposal** - All information, in any format, destroyed from any location must have due regard to confidentiality of our employees, volunteers and service users. Paper documents should be shredded, including the use of confidential shredding systems where required. CD-ROMs should be physically destroyed when they are no longer required. Electronic files on PCs and work mobiles etc. should be deleted as appropriate and the recycling bin emptied. When computers are disposed of, no personal or sensitive data is left on the hard drive and secure disposal of the computer or hard drive should be arranged. When records or data files are identified for disposal are destroyed, a register of such records needs to be kept.

Data retention

CRCC will not keep the personal data of service users and workers for longer than is necessary for the purposes set out in this policy. When that information is no longer required, we will ensure it is disposed of/deleted from our systems in a secure manner at the appropriate time in accordance with the current statutory and recommended regulations.

Roles and responsibilities

All staff, sessional staff and volunteers within the organisation have a responsibility to ensure the processes and procedures detailed in this policy and related policies (detailed previously) are adhered to.

Board level responsibility for overseeing and managing information risk within CRCC sits with the Senior Information Risk Owner (SIRO). The role is filled by a member of CRCC's Board of Trustees. The SIRO ensures that CRCC has affective systems and processes in place to address information governance and information security risk, acting as the overall owner of information risk.

Day-to-day responsibility for monitoring CRCC's compliance with data protection laws, particularly the UK and EU GDPR, sits with the Data Protection Officer. They advise on data protection obligations, conduct Data Protection Impact Assessments (DPIAs) and serve as a point of contact for individuals and data protections authorities.

The current Senior Information Risk Owner for CRCC is:

Jenny Grech (Trustee Secretary)

The current Data Protections Officers for CRCC are:

Norah Al-Ani (Director) and Clare Baker (Centre Manager)

Multi-agency information sharing principles and protocols

The Home Office has issued guiding principles for multi-agency information sharing, which includes the following checklist for practitioners:

- Has the service user been informed of the reasons why their data may be shared?
- Has the service user been informed of what information may be shared, when and with whom?
- Has the service user been reasonably informed of the implications of their granting consent?
- Has the service user been informed of their right to refuse consent, give partial consent (i.e. allow the sharing of some information) or withdraw it at any time?
- Have measures been put in place to ensure that the service user will be kept up-to-date with the information sharing process in relation to their information?

Appropriate translation services need to be provided if service users are unable to communicate in English. Other communication issues for example, having low literacy levels, will also need to be taken into consideration and provision made for the service user. Agencies must find a way of ensuring the service user is able to communicate as this is a key part of providing a survivor-centred and culturally sensitive service.

Each service user's needs should be assessed on an individual basis and additional steps taken such as the publication of information in a range of languages, use of translators, and/or involvements of advocates to ensure that service users can give informed explicit consent.

Formal information sharing protocols

CRCC operates within a multi-agency setting, playing a key role in strategic and operational initiatives. Some of these partnerships are underpinned by formal data sharing protocols, to which CRCC maybe a signatory.

In these cases, it is CRCC's duty to share information as required under these protocols. If a staff member or volunteer has concerns about sharing data in these circumstances these should be initially discussed with the Director; and, if not resolved, with the Chair of Trustees or other member of the Board.

Service users' data

CRCC is committed to providing respectful and safe services to all its service users and aims to create a transparent and lawful decision-making process when sharing information regarding service users, which prioritises the safety of service users, staff, volunteers, the services and the charity.

This is best achieved when:

- CRCC works with the consent of service users to share information with other agencies and/or agencies.

- CRCC creates a safe environment for service users to share information so that it can act in their best interests.

- CRCC services have considered and understand the threshold surrounding sharing confidential information entrusted to it when acting to protect service users and their children.

- CRCC clearly explains why it collects information, how it will use this information, how it will be kept secure and how boundaries to confidentiality apply.

In general, all information about service users, their lives, families and others given by service users and other agencies to CRCC services will be treated as confidential:

- Workers should only discuss details of service users on a need-to-know basis both internally and externally, and never with other service users.

- In relation to record keeping of service users' confidential information; a separate section within the file should be kept for third party information.

- At times, CRCC provides group activities for service users which contribute to their health and wellbeing. At the end of each group, service users must be reminded that any details of individuals' circumstances, which have been shared, should remain confidential.

- Any reports (internal or external) should not identify service users unless specifically required. Initials should be used. If the report writer feels that this information should be disclosed, it should be discussed with the Director.

- All communications (internal and external) should not identify service users unless specifically required. Initials or first names should be used. If the employee or volunteer feels that this information should be disclosed, it should be discussed with the Director.

Confidentiality statement and gaining informed consent to share information

In gaining consent:

- Workers must be clear with the service user about why they want to share information about them and who it will be shared with;
- Service users should have a chance to put their point of view and to ask any questions;
- Such discussions should be recorded and service users should be asked to sign a consent form where practicable (see below);
- Where the service user refuses consent, a record should also be kept. Where this is the case, if workers have grounds to share the information without the service user's consent and intend to do so, they should tell the service user of their intention unless there are good reasons not to do so, such as jeopardising someone's safety;
- All such records should be kept on an individual's file.

A confidentiality and information sharing statement must be made available to service users and explained to every service user in a way appropriate to the service and the individual. This will explain how we will store and use a service user's information as well as the requirements to ensure confidentiality, and how confidentiality relates to the sharing of information with and without consent.

Unless obtaining written consent is not possible or impracticable (e.g. in telephone-based support services), service users will be asked to sign a confidentiality statement. In most cases, consent can be sought when service users first come into contact with the charity. However, CRCC workers may encounter service users when they are emotionally distraught, disorientated and/or physically injured and it may not be possible to obtain explicit consent to share information at this time. Professional judgement will come into play in making an assessment as to when would be a good time to seek consent.

Where verbal consent is sought, the following should be noted in the service user's file:

- The time, date and identity of the person seeking the consent are recorded;
- The decision of the service user is recorded; (e.g. 'Consent Given'. 'Consent Denied'. 'Consent Not Sought'. Any other advice or action taken should also be recorded);
- Relevant action such as any disclosure of information taken following the granting of consent is recorded;
- Access to all information stored on service users will be limited to those working for or on behalf of CRCC.

In situations where the service user, their children and/or others are assessed as being at high risk of harm, CRCC will act to secure their protection taking all reasonable means to ensure this is done with their consent. This could also be without the consent of the service user, in adherence with this policy and legislation, and staff will need to consult with the Director when this situation arises. The possibility of this situation occurring should be explained to service users at intake into the service.

Withdrawal of consent

Service users are entitled to withdraw their consent to the sharing of information at any point during assessment or provision of services. The service user must be informed that they can exercise this right and that, should they do so, they will be informed of any potential impact on service delivery.

In the event that an individual withdraws their consent for their personal information to be shared, or wishes to subsequently place/amend restriction upon the personal information to be shared, the agency receiving such a request will immediately inform all other agencies who are, or may be, affected and record the details on the individual's file.

In the case of consent being withdrawn, no further personal information should be disclosed unless there are statutory reasons for doing so, or legal exemptions can be applied.

Sharing information with consent

Service users have a right to know that the information they share with CRCC will remain confidential and only be disclosed with their consent, or if the organisation believes that the service user is at significant risk of causing harm, either to themselves or others.

Where consent from the service user is sought, they must understand:

- why this information needs to be shared
- with whom the information is shared
- what are the potential consequences of both sharing and not sharing this information
- that consent can be withdrawn at any time.

If they consent, this must be signed, documented and put on their case file (in accordance with the above).

Sharing information without consent

It is CRCC's duty to safeguard service users, both adults and children, and this may require the sharing of information without the service user's consent. If the service user does not consent to sharing the

information with other parties, the reasons for this should be formally documented in their case notes or on call recording systems.

Where it is felt that information needs to be shared in order to keep a service user safe, the Director should be informed where there is a clear need to share this information without consent. These decisions also require reference to the 'Safeguarding Children and Adults at Risk Policy'.

CRCC workers should inform the service user that information is being shared without their consent and, if possible, encourage them to share the information themselves. The possibility of this situation occurring should be explained to service users at intake.

In exceptional circumstances, if it is considered that informing the service user about information sharing without their consent will/could put the service user, their children and/or others at increased risk, the worker should discuss with their line manager. If it is agreed that there is an increased risk, the discussions and the decision not to inform the service user should be noted on the case file. Any potential risk to the worker should also be discussed and the appropriate action taken.

If a decision is made to share information without consent (whether this is with or without the service user's knowledge) then the worker should note the reasons clearly in the case file. This should include whether the service user has/has not been informed and the reasons for this and reference the 'Safeguarding Children and Adults at Risk Policy'.

When information is shared, workers will follow the specified procedures for information sharing that only allow the disclosure of sufficient information to enable the relevant agencies to carry out their duties.

Sharing sensitive personal data without consent

In sharing 'sensitive personal data' without consent (i.e. physical or mental health condition, racial or ethnic origin, political opinions, trade union membership, religious life, sexual life, criminal offences, gender identity), one of the following MUST apply:

- It is necessary to establish, exercise or defend legal rights.
  -OR-
- It is necessary to defend someone's vital interests (life and death situations and serious and immediate concerns for someone's safety) and the person to whom the information relates:
  - cannot consent (e.g. a very young child)
    -OR-
  - is unreasonably withholding consent
    -OR-
  - consent cannot reasonably be expected to be obtained.
    -OR-
- It is necessary to perform a statutory function that applies to your organisation under an act of parliament.
  -OR-
- It is in the substantial public interest and necessary to prevent or detect an unlawful act and obtaining consent would prejudice this purpose (e.g. if someone is at high risk of harm).

Sharing non-sensitive personal data without consent

In sharing non-sensitive personal data without consent, one of the following MUST apply:

- The information does not allow the individual to be identified.
  -OR-
- The need to protect a person's 'vital interest' overrides the need for confidentiality – this generally applies to life and death situations and serious and immediate concerns for someone's safety.
  -OR-
- You are required to do so by a court order.
  -OR-
- You have a legal duty to do so via legislation or related guidance that has legal status.
  -OR-
- It is necessary to prevent or help detect a crime.
  -OR-
- It is necessary for the legitimate interests of the person sharing the information, unless to do so would conflict with the rights, freedom and legitimate interests of the person the information is about.

Considerations when supporting children and young people

A parent or legal guardian's consent can be overridden in respect of safeguarding the interests of children, although, where possible, it would be helpful to gain their consent or/and keep them informed of actions. The 'Safeguarding Children and Adults at Risk Policy' reinforces this approach.

With regard to gaining a child's consent in sharing information about them, the Data Protection Act 2018 does not set down a precise age at which a child can act in her/his own right. However, there is a general adoption of the principle that consent should normally be gained from a parent/legal guardian unless the child is over 12 and clearly understands what is involved and is capable of making an informed decision.

In some situations, where gaining consent from the parent/guardian may exacerbate a situation of actual or threatened harm to a child, their consent will not be sought. It is, therefore, possible that in some circumstances action may be taken where consent has not been gained from the adult or child (i.e. where the child is under 12 or over but without the capacity to understand). Where this takes place, workers will ensure that the process and any actions are fully recorded.

If an adult is granting consent on behalf of a child, the person granting consent must have parental rights. In cases where parents are separated, the consent will usually be sought from the parent with whom the child resides. If the child is subject to a Care Order then the local authority will share parental rights for them with their parents.

In principle, where it is possible, a child's consent should be gained for sharing information about them. Where it is not possible to achieve informed consent they must be listened to, consulted and informed in general about what is happening. The communication must be sensitive and reflect a child's ability to comprehend.

Transfer of data to other agencies

When staff members are required to share information with outside bodies they must ensure that they observe the steps set out below, in addition to any requirements contained within multi-agency information sharing protocols (e.g. for MARACs and Safeguarding services):

- the information must go directly to the right person, making sure that the information is marked private and confidential and, if it is a fax or email, make sure that the person is in the right place at the right time to receive this;

- make sure that they know who, if anyone, the information will be shared with by the recipient;

- they will ensure that the recipient understands the sensitivity and status of that information and knows what to do with it;

- they will ensure that the sharing of information is a private not public process;

- they will communicate with that person to ensure they understand the next steps and any further action;

- if the member of staff feels that as a consequence of sharing information, a staff member or service user may be at risk, this must be discussed with their line manager or a member of the Senior Leadership Team and the information can be shared so long as the circumstances set out above are satisfied.
- where possible an information sharing protocol should be established with outside organisations with whom regular or repeated sharing is possible.

Employee, trustee and volunteer data

All CRCC employees, trustees and volunteers will receive a copy of this policy as part of their induction and training.

Data about employees, trustees and volunteers may be processed for legal, personnel, administrative and management purposes and to enable CRCC to meet its legal obligations as an employer, for example to pay staff, monitor their performance and to confer benefits in connection with their employment.

Examples of when sensitive personal data of staff is likely to be processed are set out below:

- Information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work.
- The employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation.
- To comply with legal requirements and obligations to third parties.

Subject Access Requests (SARs)

Individuals have the statutory right to access and receive a copy of their personal data and other supplementary information. This is commonly referred to as a subject access request or 'SAR'. It helps individuals to understand how and why the charity are using their data, and check we are doing it lawfully.

Individuals can make SARs verbally or in writing, including via social media. A request is valid if is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.

In most cases, CRCC cannot charge a fee to comply with a SAR. However, CRCC can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their data.

Timescale

CRCC must comply with a SAR without undue delay and respond to a SAR within one calendar month of receiving the request. The timescale for responding to a SAR does not begin until CRCC has received ID confirmation and the charity should request any ID documents promptly.

The charity may extend this time to respond by a further two months if the request is complex or we have received a number of requests from the same individual, in which case we will notify the requester within the first calendar month.

Any staff member who receives a SAR should forward it to their line manager immediately. In the line manager's absence, the Director or Centre Manager should be sent the request.

Verifying identity

Staff members should always quickly satisfy themselves as to the identity of a person making a SAR. Staff members shouldn't ask for formal ID unless it's necessary and proportionate. Instead, they could ask questions that only that person would know, such as appointment details, or for ID documents that they can verify.

Anyone can authorise a third party to help them with a SAR, and it should be enough to verify this by having a letter from the person nominating the individual as their representative.

If employees have reason to believe that someone is falsely claiming to act on behalf of a person making a SAR, this should be reported to their line manager and be investigated before any information is disclosed.

Searching for the relevant information

Staff members should check the request carefully to ensure they are clear about what information is being asked for by the requester. The individual may be asking for all information we have, or for data relating to one particular thing, and the staff member may check with the individual if it is unclear.

CRCC will make all reasonable efforts to find and retrieve the requested information. However, we are not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

Supplying the requested information

Requested information will generally be provided in the format asked for by the requester.

If the requester is a service user, due to the sensitive nature of CRCC's work, where possible the service user should be offered an appointment to review the information with the relevant line manager, so that the line manager can answer any questions or concerns they may have.

Recording SAR handling

All SARs should be recorded appropriately, and include the time and date the request taken and time it took to deal with the request. These records should be kept for a period of at least one year.

Staff members should keep a record of exactly what information has been provided in response to a SAR, together with a note detailing anything withheld and/or amended; this should include notes relating to how they reached these decisions and notes on any exemptions relied on. These notes should also be kept with this record.

Keeping records on SAR handling will allow CRCC to determine what information should be disclosed if a further SAR is received in the future and it will also help if CRCC needs to explain or justify the decisions made in respect of any SAR.

Exemptions

Exemptions to disclosure apply to any information that is processed for purposes concerned with:

- Crime and taxation, where the disclosure might prejudice those purposes.
- Negotiations, where the data comprises records of the intentions of an organisation that is negotiating with the requester.
- Health, where in the opinion of a health professional disclosure might cause harm to the requester.
- Adoption records relating to the requester.
- Legal professional privilege.
- Any matter where there is a substantial public interest in not disclosing the information.

These examples are those most likely to apply in practice but there are other exemptions to disclosure detailed in the Data Protection Act 2018 that may be relevant when dealing with a SAR. For more information, please see the ICO's guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/

Special cases

There are also special rules and provisions about SARs and some categories of personal data, including:

- unstructured manual records;
- credit files;
- health data;
- educational data; and
- social work data.

For more information, please see the ICO's guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/are-there-any-special-cases/

Refusing a request

Where an exemption applies, CRCC may refuse to provide all or some of the requested information, depending on the circumstances. We can also refuse to comply with a SAR if it is manifestly unfounded or manifestly excessive.

If we refuse to comply with a request, the staff member must inform the individual of:

- the reasons why;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through the courts.

Service user case notes

If a service user requests to see their cases notes:

- This should be noted on their file and the relevant line manager should be informed immediately.

- The case notes will be reviewed to see if they contain a recent professional's opinion. If so, then the professional should be contacted for consent to disclosure, where it should be explained that the final decision rests with CRCC. This process must be recorded.

- If it is not possible to consult the professional concerned, or the opinion is historical, then the information should be anonymised.
- Any objections a professional makes to disclosure should be carefully considered; particularly, if there is a real risk that disclosure of this information would be likely to cause them, or any other individual, harm.

- CRCC will provide a response to a subject access request within one calendar month of receiving the request.

- Due to the sensitive nature of CRCC's work, where possible, the service user should be offered an appointment to review the information with the line manager, so that the line manager can answer any questions or concerns they may have.

- Service users who are parents may also view information about their children (unless to do so would place the child in a situation of potential or actual harm). Where this occurs when the child/young person is deemed competent, their permission should be sought. There is no single test for determining a young person's competence.

  However good practice guidelines recommend considering the following when assessing competence:

  - ability to understand that there is a choice and that choices have consequences
  - willingness and ability to make a choice (including the option that someone else make decisions for them)
  - understanding the nature and purpose of the proposed service
  - understanding the alternatives to the service
  - freedom from pressure

In addition, there is no legal decision that sets a minimum age at which children can be regarded as competent to consent. However, it is unlikely that many children under the age of 12 would be deemed competent.

Staff personnel files

If a staff member requests to view their personnel file:

- Their line manager will review the file to check if it identifies colleagues who have contributed to, or been discussed in the file; and
- where those individuals do not consent to being identified, those details may be anonymised.

If a subject access request cannot be complied with, without releasing personal data, then the request does not have to be complied with, unless the third party has consented, or it is reasonable in all the circumstances to comply with the request without such consent.

Further information

Further information in relation to SARs and how to respond can be found on the ICO website: https://ico.org.uk/for-organisations/advice-for-small-organisations/how-to-deal-with-a-request-for-information-a-step-by-step-guide/

General issues in respect of confidentiality and the work of CRCC

When workers are discussing service users amongst themselves, discussing a service user with another agency on the telephone or when service users visit CRCC's offices, they must:

- Make sure any discussion happens in an appropriate place, e.g. not in an office where other staff are working or where people are coming in and out of the place.

- Not gossip about service users with other service users, staff, volunteers or trustees.
- Not discuss personal facts about one service user with another service user or in the presence of another service user.

- Not make or write judgemental, victim-blaming or derogatory comments about service users in their files or anywhere else.

- Not leave information lying around or on screen but replace it in the appropriate place (locked filing cabinets).

When making calls with agencies, contacting service users, and leaving messages on external phones:

- Any staff member dealing with enquiries from third parties should not disclose any personal information held by CRCC about service users.

- Telephone messages should not be left on the phones of people referred to the service unless it is absolutely certain that CRCC has a safe contact number for them.

- If a number is recorded as 'safe' on the referral form, staff should bear in mind that survivors circumstances can change quickly e.g. what was safe when the police attended an incident may not be safe several days later.

- When telephone messages are left on service users' voicemails these should contain minimal details.

- Workers should never leave personal details about service users on other agencies answer machines. Any messages left should contain minimal details.

Under no circumstances should the work of CRCC be discussed in a non-professional situation outside of the working environment. This includes general conversation with work colleagues, friends and family.

Under no circumstances should the identity of service users or previous service users be discussed in a non-professional situation outside of the working environment. This includes general conversation with work colleagues, friends and family.

Information on service users and/or women and children, will be shared between workers and with outside bodies within the framework set out previously. Where information is given to outside agencies or other individuals, workers will always ensure that they are certain that the individual is who they claim to be before disclosing any information. The same requirements apply in relation to former service users.

Under no circumstances will any personal information relating to workers or trustees be given to any individual or organisation without the permission of that person.

All of the above will be informed about the systems, processes and protocols for keeping and using personal data that is being held about them when they first come into contact with the charity.

Emotional support services workers should never give away personal information to service users, except for their name or line-name.

Under no circumstances will current workers and trustees discuss service users, or CRCC policies and procedures with former colleagues who have left the organisation. All volunteers, staff members and trustees must continue to maintain confidentiality about service users and CRCC policies and procedures after leaving the charity. This includes maintaining the anonymity of emotional support services volunteers, both during their time as a volunteer and after they have left the organisation.

The location and address of the office should only be disclosed when necessary. The PO Box should be used for most correspondence.

Staff members must ensure that all equipment owned by CRCC, including correspondence files, are kept secure, including all CRCC property in transit. Laptops must be kept secure whilst travelling and within the home. CRCC will require the employee to certify that they are able to maintain security and confidentiality of documents within the home and comply with IT security and data protection requirements. CRCC reserves the right to take all reasonable steps necessary to verify this.

CRCC requires staff to take reasonable precautions to safeguard the security of equipment, and keep passwords secret.

Staff members should, as appropriate, inform the police and the Director or Centre Manager as soon as possible if either a CRCC laptop or work mobile in your possession or any computer equipment on which CRCC work is undertaken (even if this is personal IT or ICT equipment) has been lost or stolen.

Staff members should ensure that all laptops are regularly backed up.

All desks should be left clear of equipment and paperwork at the end of each working day/shift and all cupboards should be locked.

Training

All workers and trustees will be trained in the use of this policy and procedure to ensure that confidentiality and access to information are dealt with appropriately at all times.

All staff will receive training in data protection to comply with the Information Commissioner's Office registration.

Breach of policy and confidentiality

Where there is evidence that a worker has knowingly divulged confidential information regarding service user(s), worker(s) and/or trustee(s), immediate action will be taken under the 'Disciplinary and Grievance Policy' (with advice from HR advisors, Peninsula, where necessary) and the Director and/or Chair informed, as appropriate.

If there is an allegation that a worker has knowingly divulged confidential information regarding service user(s), worker(s) and/or trustee(s), the Director will carry out a fact-finding investigation and submit a report to the trustees by the next meeting. If the allegation is found to be accurate, then action will be taken under the 'Disciplinary and Grievance Policy'.

Where there is evidence that a trustee has knowingly divulged confidential information regarding service user(s) or worker(s), an emergency trustees' meeting will be called within two weeks.

If there is an allegation that a trustee has knowingly divulged confidential information regarding service user(s) or worker(s), the matter will be reported to the Chair of Trustees or the entire Board of Trustees. if the allegation is made against the Chair. The trustees will appoint an individual to carry out a fact-finding investigation and submit a report by the next meeting, or present it directly to the Chair or Deputy Chair for action, if the fact-finding has highlighted issues of potentially serious consequence to CRCC.

The paramount need to maintain confidentiality and to maintain safety will be explained to women and children when they first receive services from the charity, through a range of relevant paperwork such as the Confidentiality and Consent Agreement, Service Guides, Service Agreements and will be reinforced on a regular and appropriate basis.

Complaints

The 'Service User Complaints Policy' or the 'Fundraising Complaints Policy' should be referred to in the first instance.

If there is a breach of confidentiality and/or the Data Protection Act 2018, any individual or organisation can make a complaint to the Information Commissioner Office about CRCC. This could have serious consequences for the charity, in addition to any adverse consequence for the service user or other individual.

The Information Commissioner in the first instance will work with CRCC to rectify any breaches, but has the power to issue enforcement notices and, if those are ignored, can choose to prosecute and levy fines.

Information to the police and other investigating agencies

There is no legal duty to disclose information to the police without a police warrant, Court Order or a DP1 Form (sometimes referred to as a Section 29 (3) Form) although withholding information could be deemed to be obstructing the police.

A DP1 Form must be signed by a Superintendent. If such a document is produced it should be received by the relevant service manager or, in their absence, the Director.

Where CRCC is approached to disclose information to the police with or without such documents, or where another investigative agency makes a request, staff members must follow the charity's 'Third Party Notes Request Process'.

Pressure from the police to reveal personal information about a service user is considered inappropriate and CRCC will consider making a complaint to the relevant authority.

Requests are likely to be declined if they are deemed by CRCC to be inappropriate. Repeated inappropriate requests by particular individuals or agencies will be reported to the Information Commissioner's Office (ICO).

Any decision to disclose information to the police must be made by the appropriate staff member and in consultation the service user. It must be remembered that disclosure of information, other than as outlined in the exemptions, cannot be done without the service user's consent. If the service user's consent cannot be obtained, CRCC will not disclose information to the police unless a court orders CRCC to do so.

If the police are convinced that they need information that is being held by CRCC, they can apply to the courts for a witness or search order.

A witness summons is a formal and legally binding order of the court to attend court and give evidence. In some instances, the court will require you to bring certain documents with you. If this is the case the summons will make it clear what documents are needed.

A witness summons is legally binding on the person or persons named on the document and a failure to attend court when summonsed can be treated as 'a contempt of court' punishable by a fine or imprisonment. (HMRC)

If CRCC or one of its workers or trustees receives or is served with a witness summons, they must follow the charity's 'Court Summons Policy'.

Third parties

Sometimes someone claiming to be a relative or solicitor of a service user may contact the charity asking to have information forwarded or to be put in touch with the service user.

Under no circumstances should workers comment on whether or not the individual is a service user of a particular CRCC service or the charity as a whole. Staff must suggest the third party puts their request in writing to the Director and the procedures set out in the 'Third Party Notes Process' document must be followed.

Exceptions to this apply where:

- the service user is prepared to allow this in which case their written authorisation is required, or prevention of terrorism;
- significant risk of harm to children or young people;
- serious risk of harm to adults.

Policy Version: Version 3

This policy was reviewed and ratified by the Board of Trustees on the 4 June 2024.
This policy was reviewed and amended (NAA/CB by trustee delegation) on the 4 June 2025.
This policy will be next reviewed by the 4 June 2028.

Cambridge Rape Crisis Centre
Box R, 12 Mill Road, Cambridge CB1 2AD
T: 01223 313 551 | E: contact@cambridgerapecrisis.org.uk | W: cambridgerapecrisis.org.uk
Registered Charity No. 1179871