Cambridge Rape Crisis Centre:
Confidentiality, Data Protection and Sharing Information Policy

Contents

Purpose

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 (among 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 wellbeing 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 staff to access information, which 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 organisation has ended.

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

- General Data Protection Regulations 2018
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Children Act 1989
- The Crime and Disorder Act 1998

Related policies: Child Protection Policy, Vulnerable Adults Policy and Confidentiality Policy.

Definition of terms

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 1998 and the General Data Protection Regulations 2018, workers, 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 protection**. All data is kept confidential using passwords for electronic records and locked filing cabinets for paper records. All data must be cleared from desks and locked

away each evening. Password information should be kept by each individual and not disclosed to any other person inside or outside the organisation.

- **Equipment**. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- **Authorised removal**. Client case files 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.
- **Methods of disposal**. All information, in any format, destroyed from any location must have due regard to confidentiality of our employees, volunteers and clients. 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 laptops 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: All staff personnel files will be kept by CRCC at our offices and access will be limited to designated managerial staff, relevant trustees and the individual concerned. When an individual leaves their supervision notes will be destroyed after six months. The remaining file will be destroyed after six years.

Disclosure and Barring Scheme (DBS) checks will be undertaken on employees and volunteers where relevant, which involve asking employees and volunteers to see their certificate. The employer can keep copies of these, with the applicant's consent. The same data protection provisions must be applied when keeping a copy of the certificate. These will be stored separately from staff personnel files and in accordance with the DBS Code of Practice and Employer Guidance.

CRCC will not keep the personal data of service users for longer than is necessary for the purpose. We will destroy or erase such data from our systems six years from the date of last entry (see appendix on recommended retention periods).

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 client been informed of the reasons why their data may be shared?
- Has the client been informed of what information may be shared, when and with whom?
- Has the client been reasonably informed of the implications of their granting consent?
- Has the client 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 client will be kept up-to-date with the information sharing process in relation to their information?

Appropriate translation services need to be provided if clients 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 client. Agencies must find a way of ensuring the client is able to communicate and this is a key part of a providing a client-centred and culturally sensitive service.

Each client'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 clients 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 clients and aims to create a transparent and lawful decision-making process when sharing information regarding clients, which prioritises the safety of clients, staff, volunteers, the service and the organisation.

This is best achieved when:

- CRCC works with the consent of clients to share information with other agencies and/or agencies.
- CRCC creates a safe environment for clients 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 clients 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 clients, their lives, families and others given by clients and other agencies to CRCC client services will be treated as confidential.

- Staff and volunteers 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.
- CRCC at times 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.

Confidentiality statement and gaining informed consent to share information

In gaining consent:

- Staff and volunteers must be clear with the client about why they want to share information about them and who it will be shared with
- clients should have a chance to put their point of view and to ask any questions
- such discussions should be recorded and clients should be asked to sign a consent form where practicable (see below)
- where the client refuses consent a record should also be kept. Where this is the case if staff or volunteers have grounds to share the information without the client's consent and intend to do so they should tell the client 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 clients and explained to every client in a means appropriate to the service. This will explain how we will store and use a client'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), clients will be asked to sign a confidentiality statement. In most cases, consent can be sought when clients first come into contact with an organisation. However, many frontline service providers encounter clients 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, this should be noted in the client file:

- the time, date and identity of the person seeking the consent are recorded
- the decision of the client 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 clients will be limited to those working for or on behalf of CRCC.

In situations where the client, 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 be without the consent of the client, 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 clients at intake into the service.

Withdrawal of consent

Clients 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 her 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 clients 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 Child Protection policy and the Vulnerable Adults policy.

CRCC employees and volunteers should inform the client 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 clients 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 staff member 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 staff member 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 staff member should note the reasons clearly in the client file. This should include whether the client has/has not been informed and the reasons for this and reference the Child Protection policy and the Vulnerable Adults policy.

When information is shared, staff and volunteers 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.

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 some is at high risk of harm).

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 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

It is clear from the above that a parent or legal guardian's consent can be overridden in respect of safeguarding the interests of children – although as set out below, where possible, it would be helpful to gain their consent or/and keep them informed of actions. The Child Protection policy and procedures reinforce this approach.

With regard to gaining a child's consent in sharing information about them, the Data Protection Act 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, staff 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 abilities to comprehend.

Transfer of data to other agencies

When members of staff 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 e-mail 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 another service user may be at risk, this must be discussed at management level within the organisation 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.

Trustee, Employee and Volunteer data

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

Data about Trustees, employees and volunteers may be processed for legal, personnel, administrative and management purposes and to enable advance 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)

Section 7 of the Data Protection Act 1998 (the Act) and the new General Data Protection Regulations 2018 gives individuals the statutory right, subject to some exemptions, to see information which organisations hold about them. SARs must be made in writing and accompanied by the statutory fee, if charged, currently set at a maximum of £10. There is a 40-day statutory maximum period allowed for responding to a SAR.

All SAR should be recorded appropriately, include time and date request taken and time it took to deal with the request. These records should be kept for a period of at least one year.
A data subject (whether staff member or service user) has a right, on making a request to CCRC, of being informed whether their personal data is being processed by or on behalf of the charity.

If it is, then the data subject also has a right to:

- a description of the personal data held, the purposes for which it is being processed and the recipient or classes of recipient to whom the data may be disclosed, and
- any information available to CRCC as to the source of the data (subject to certain stated confidentiality protections for individual sources).
- A subject access request must be made formally in writing. Any staff member who receives a written request should forward it to their manager immediately.

Verifying identity

Staff should always satisfy themselves as to the identity of a person making a SAR. Anyone can authorise a representative 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 manager and be investigated this before information is disclosed.

Recording SAR handling

Staff should keep a record of exactly what information has been provided in response to a SAR, together with a note of information of 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 comprise records of the intentions of an organisation that is negotiating with the Subject
- Health, where in the opinion of a health professional disclosure might cause harm to the Subject
- Adoption records relating to the Subject
- Legal professional privilege
- Any matter where there is a substantial public interest in not disclosing the information.

Further information in relation to subject access requests and how to respond can be found on the ICO website:
http://www.ico.gov.uk/for_organisations/data_protection/subject_access_requests.aspx

If a service user requests to see their case 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 40 calendar days of receiving it (statutory maximum), or earlier if possible.
- 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 manager, so that the 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 where 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.

If a staff member requests their personnel file:

- the 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.

General issues in respect of confidentiality and the work of the organisation

When staff or volunteers are discussing clients amongst themselves/discussing a client with another agency on the telephone/when clients 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 clients with other clients, staff or Trustees.
- Not discuss personal facts about one client with another client or in the presence of another client.
- Not make or write judgemental, victim-blaming or derogatory comments about clients in their files or anywhere else.
- Not leave information lying around or on screen but replace it in the appropriate place (locked filing cabinets).

Calls from agencies, contacting clients, 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 clients.
- 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.
- Where telephone messages are left on clients answer machines these should contain minimal details.
- Staff and volunteers should never leave personal details about clients 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 clients or previous clients 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, women and children, will be shared between staff, volunteers, Trustees and with outside bodies within the framework set out above. Where information is given to outside agencies or other individuals, members of staff 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 staff members, volunteers 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 organisation. Helpline and email workers should never give away personal information to callers or emailers, except for their name or line-name.

Under no circumstances will current volunteers, employees 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 organisation. This includes maintaining the anonymity of

Helpline and Email Workers, 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; inform the police and the Director (as appropriate) as soon as possible if either a CRCC laptop in your possession or any computer equipment on which CRCC work is undertaken (even if this is personal IT equipment) has been lost or stolen; and 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 staff members, volunteers 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 of confidentiality

Where there is evidence that a Staff member or volunteer has divulged confidential information on a service user/s or member of staff; immediate action will be taken under the Disciplinary Policy, with advice from HR advisors Peninsular where necessary, and the Director/Chair informed as appropriate.

If there is an allegation that a staff member or volunteer has divulged confidential information on a service user/s or staff member: the Director will carry out a fact finding investigation and submit a report to the Trustees by the next meeting; and if the allegation is found to be accurate, then action will be taken under the Disciplinary policy.

Trustees: Where there is evidence that a trustee has divulged confidential information on a service user/s or member of Staff, an emergency trustees' meeting will be called within two weeks. If there is an allegation that a trustee has divulged confidential information on a service user/s or member of staff, the matter will be reported to the chair of trustees; or the entire board 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/Deputy-Chair for action if the fact finding has highlighted issues of potentially serious consequence to CRCC.

Service users: The paramount need to maintain confidentiality to maintain safety will be explained to women and children when they first receive services from the organisation 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 CRCC Complaints Policy should be referred to in the first instance.

If there is a breach of confidentiality/the Data Protection Act, any individual or organisation can make a complaint to the Information Commissioner about CRCC. This could have serious consequences for the organisation in addition to any adverse consequence for a client. The Information Commissioner in the first instance will work with an organisation 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 Manager.

Where CRCC is approached to disclose information to the Police without such documents, or where another investigative agency makes a request, staff must:

- explain the confidentiality policy
- ask for the legal basis of the request for information
- refer the matter to the Manager.

Should a police officer enter the building, they should not be taken into a room where records are kept and the CRCC confidentiality procedure should be explained to them immediately.

- Pressure from the police to reveal personal information about a client is considered inappropriate and CRCC will consider making a complaint to the relevant authority.
- Any decision to disclose information to the police must be made by with 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 client's consent. If the client's consent cannot be obtained, CRCC will not disclose information to the police.
- 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 volunteers, employees or trustees receives or is served with a witness summons, the Chair should be informed, or in their absence the Deputy Chair, who is then responsible for informing all other trustees promptly and will then ensure that the following steps are taken:

1. CRCC's policy in relation to confidentiality and the disclosure of information. Wherever possible it will also contain a request that the witness summons is set aside.
2. Notify the affected service user immediately of the witness summons and the need to comply. Ensure that the service user understands what a witness summons is and CRCC's duty to reveal truthful and accurate information to the Court.
3. Where possible obtain written consent from the service user allowing CRCC to disclose information to the Court.
4. CRCC will keep the service user informed of the developments with respect to CRCC (or its representatives)
5. CRCC will, where necessary, seek legal advice in relation to the witness summons and the requirements contained therein.

Third parties:

Sometimes someone claiming to be a relative or solicitor of the service user may contact the organisation asking to have information forwarded or to be put in touch with the service user. Under no circumstances should staff or volunteers comment on whether or not the client is a service

user of the service or other organisation. Staff must suggest the third party puts their request in writing to the Director and the procedures set out above should 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

Appendix I: Statutory and Recommended Retention Periods

Statutory retention periods

Record	Statutory retention period	Statutory authority
Records relating to children	until the child reaches the age of 21 or until the child reaches 24 for child protection records	Limitation Act 1980
Accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894

Recommended Retention Periods

Record	Recommended Retention Period
Client records (if no children)	Up to 6 years from the date that the client leaves the service, in case of litigation for negligence
Application forms and interview notes (for unsuccessful candidates)	At least 1 year
Assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	Permanently
Inland Revenue approvals	Permanently
Money purchase details	6 years after the transaction or value taken
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy
Trustee minutes	Permanently
accident books, accident records/reports	3 years after the date of the last entry

Appendix II: Legislation

The Data Protection Act 1998 All information and data which can identify a person, held in any format (visual, verbal, paper, computer, microfilm etc.) is safeguarded by the Data Protection Act 1998 (DPA 1998). Contained within the Act are eight principles of good practice:

1. Personal data shall be processed fairly and lawfully.
The principle is often considered the most difficult to satisfy – data must be processed fairly. Processing applies to everything we do with data, from collecting and storing, to retrieving, organising and destroying it. For the processing to be fair there should be no surprises; data subjects (service users, clients and staff) must be told why their information is collected, what an agency intends doing with it, with whom they may share it and who the Data Controller is. This is done via 'fair obtaining notices' and information leaflets. They should also be provided with further information, such as the consequences of the processing, and must not be deceived or misled as to why the information is used.
When working in a team, staff should ensure that the service user / client is aware of the members of the team and that all those involved with their care may need to see their notes / records.
To be lawful, personal information must not be processed unless:
a. at least one of the conditions in Schedule 2 of the DPA 1998 is met, and
b. in the case of sensitive data, at least one of the conditions in Schedule 3 of the DPA 1998 is also met. The DPA 1998 makes specific provision for sensitive personal data. Sensitive data includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, criminal proceedings or convictions.

2. Personal data shall be obtained only for one or more specified lawful purpose(s), and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage, to personal data. This will include:

- password control
- lockable files / rooms
- designated, authorised staff
- procedures for the disposal of confidential material including computer media
- authentication of enquirers' identity over the telephone
- home working policy / guidance
- precautions against natural disaster an Information Security Policy

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Human Rights Act 1998

The Human Rights Act 1998 (HRA) came into force in the United Kingdom on 1 October 2000. It incorporates the rights and freedoms set out in the European Convention on Human Rights. The English Courts must take into account decisions of the European Court of Human Rights.
Relevant Articles here are:

- Article 6 - Right to a fair hearing – clients should be made aware of procedures, which enable them to see all relevant and appropriate information.
- Article 8 – Right to respect for family and private life – unauthorised disclosure of a service user / client's record is a breach of this Article, although there are cases where exceptions are likely to apply.
- Article 14 – Prohibition of discrimination – it would be in contravention of the HRA not to allow a person access to their records on the grounds of their sex, race, colour, membership of a political party etc. Also, information provided must be in a form accessible to those suffering from sensory impairments or those who cannot speak English or who may have other difficulties in understanding the information.

The Children Act 1989

Section 17, 47, and schedule 2 of the Children Act 1989 impose functions which Social Services Departments are legally obliged to undertake. In some circumstances other departments of the authority or other agencies are legally obliged to co-operate.
Sections 17 and 47 taken together impose a positive duty to safeguard and promote the welfare of children. Where there is a reasonable cause to suspect a child is suffering or is likely to suffer 'significant harm', Social Services are obliged to make all necessary enquires. Social Services are obliged to identify needs for services under Section 17. Information sharing is a crucial part of both processes.

The Crime and Disorder Act 1998

Section 115 of this act enables any person to disclose information to a relevant authority for the purpose of the prevention and reduction of crime and identification or apprehending of offenders.