

Connected Voice

Confidentiality Policy

Contents

1. Introduction
2. Definition of confidentiality
3. Connected Voice Services
4. Information about individuals
5. Information about organisations
6. Storage of confidential information
7. Connected Voice Advocacy – Maintaining Client Data
8. Processing confidential information
9. Limits to client confidentiality
10. Access to data
11. Disposal of confidential information
12. Use of client information for publicity, reporting or training purposes
13. Equity, Diversity and Inclusion
14. Meetings and gatherings
15. Training, evaluation and monitoring
16. Related Connected Voice policies

Document details and review

Reviewed: December 2024
Next review: December 2027

Circulated to: All Staff, Connected Voice Website

Frequency of review: 3 years

Signed by responsible person:



1. Introduction

This Confidentiality Policy applies to all staff, volunteers and trustees of Connected Voice. The data covered by the Confidentiality Policy includes:

- ✓ Information about Connected Voice , for example its plans or finances
- ✓ Information about other organisations
- ✓ Information about individuals, for example, clients, volunteers and staff whether recorded electronically or in paper form

All staff, volunteers, trustees and others who work at Connected Voice must respect the need for confidentiality of information held about anyone who comes into contact with the charity, and about any charity business. This is expected to continue even when contact has ceased with this person, and when the staff member, volunteer or trustee no longer works for Connected Voice.

This policy should be read in conjunction with the Connected Voice Data Protection and Information Governance Policy, ICT Policies and Procedures, Code of Conduct, Recruitment Guidelines and Systems, Flexible and Hybrid Working Policy, Equity, Diversity and Inclusion Policy, Whistleblowing Policy, Disciplinary Policy and Procedure, Safeguarding Adults Policy and Safeguarding Children and Young People Policy and Procedure.

In this policy we use the word client to refer to the individuals and organisations we work with through Connected Voice core services and our projects. We make it clear in the policy where we need to treat clients differently because of the different responsibilities we have to individuals and organisation around confidentiality and data protection.

2. Definition of confidentiality

Confidentiality is the protection of personal information. Confidentiality means keeping a client's information between you and the client, and not telling others including co-workers, friends, family, etc.

Examples of maintaining confidentiality include:

- ✓ individual files are locked and secured
- ✓ support workers do not tell other people what is in a client's file unless they have permission from the client
- ✓ information about clients is not told to people who do not need to know
- ✓ clients' medical details are not discussed without their consent
- ✓ adult clients have the right to keep any information about themselves confidential, which includes that information being kept from family and friends.

All information shared by service users, members etc is covered under this policy including:

- name, date of birth, age, sex and address
- current contact details of family, guardian etc
- bank details
- medical history or records
- personal care issues
- service records and file progress notes
- individual personal plans
- assessments or reports
- guardianship orders
- incoming or outgoing personal correspondence.

Other information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual lifestyle should also be considered confidential.

3. Connected Voice Services

Connected Voice delivers a number of services which include Support and Development, Volunteering, Business Services, Equity and Health and an Advocacy service.

Connected Voice delivers services to Voluntary, Community and Enterprise organisations as well as to individuals. This Confidentiality Policy states the procedures in place to ensure confidentiality is maintained whilst delivering these services.

Connected Voice Advocacy is a service delivered by Connected Voice and has specific requirements around confidentiality because of the nature of its work with clients. The policies, procedures and guidelines relating to maintaining client data are set out in “7” below.

4. Information about individuals

Connected Voice is committed to ensuring confidential services to all individuals. The confidentiality is between the individual and the organisation, not the members of staff delivering a particular service.

Confidential information will not be sought from a client unless expressly in the interests of that client, i.e. to enable a better service delivery.

Information will only be passed to another agency or to other individuals outside of the charity with the consent of the client, where possible this will be with written consent. If a member of staff, volunteer or trustee intends to get information from

another agency to help the client or to refer them to another agency then this must be explained to the client and their permission given.

No personal information about staff, volunteers, trustees or clients will be given to any third party including a member of the family, without the consent of the client. Information will only be divulged on a “need to know” basis. When clients lack the mental capacity to give consent/permission, advocates will work within the Best Interest Framework and a decision will be made (and recorded) in line with the Mental Capacity Act Policy.

Information will be treated in confidence and will not be divulged to anyone outside the organisation except where extenuating circumstances exist (see below). However, in order that Connected Voice can provide the best possible help to clients it may be necessary to share information with a manager or colleagues within Connected Voice.

All clients are entitled to privacy and will be made aware that they can specifically request to be seen in private.

In no circumstances should details of a client be discussed by anyone outside of the organisation or in an open plan area in such a manner that it is possible to identify the client.

Staff and volunteers should take due care and attention when speaking to clients, using the telephone or Teams. No client should be able to hear a conversation or personal details of another service user.

A private room will be used for confidential conversations with staff, clients, trustees and volunteers.

This policy has been reviewed in line with the General Data Protection Requirement which was implemented on 25 May 2018. General Data Protection Requirement will be included in the induction programme and explained regularly at staff meetings.

5. Information about organisations

The decision as to whether material relating to organisations is confidential is less clear than that relating to individuals. Connected Voice is often told a great deal about organisations that are having problems. The client organisation should be consulted as to whether this information is confidential and whether or not it can be used for research, campaigning etc.

6. Storage of confidential information

Information relating to individuals:

- ✓ Connected Voice has moved to a secure electronic storage folder system. Confidential papers are scanned and saved in a confidential client electronic folder. Access to electronic folders is only given to those staff who need access to the information.
- ✓ Confidential papers are shredded once they are scanned to the electronic folder.
- ✓ Any papers in transit are not be left on a desk or anywhere they can be viewed and will be kept in a folder in a secure place until they are scanned into an electronic client folder and then shredded.
- ✓ The line manager should be clear who has access to confidential information and who has access to the electronic folder
- ✓ Electronic case notes should only be accessed by authorised staff and be password protected
- ✓ Connected Voice database and project databases should be password protected and only accessed by authorised staff or volunteers
- ✓ Information held electronically should be password protected and only accessed by authorised staff or volunteers
- ✓ Electronic devices holding or allowing access to confidential information should be encrypted and password protected
- ✓ Connected Voice has installed a VPN line for remote working.
- ✓ Staff, volunteers and trustees working at home are instructed not to store confidential information on their home computer or devices. Staff and volunteers are given remote access to store documents into secure electronic files on the Connected Voice network. Staff, volunteers and trustees who work at home do so in line with the Connected Voice Flexible and Hybrid Working Policy.
- ✓ Confidential information sent by email is sent and received using encryption.
- ✓ The confidentiality of the recruitment process will be carried out in line with the Connected Voice Recruitment Guidelines and Systems. Application forms and information will be kept in a confidential electronic folder and only accessed by authorised staff. When the recruitment is complete documents will be kept electronically and then deleted after 6 months. E-mails relating to recruitment will only be accessed by the authorised line manager and administrator and deleted once a candidate has been appointed.
- ✓ Connected Voice has moved to keeping minimal paper personnel records. Supervision notes and appraisal forms are now stored electronically on BreatheHR. The Chief Executive, Office Manager and appropriate Line Manager are the only staff to have access to staff, volunteers or trustees

personal information. Electronic files are saved on BreatheHR and are password protected. Only authorised Line Managers have access to personnel records for their own staff. The Chief Executive and Office Manager has access to all personnel records on BreatheHR

- ✓ Payroll records are kept electronically and information stored on SAGE is only accessed by the Payroll Manager, Payroll Administrators, Head of Business Services and Finance Manager.
- ✓ Payroll records and clients' accounts that have to be kept for seven years both for Connected Voice and Business Services are kept in secure storage offsite and shredded after that time.

Information relating to Connected Voice and Connected Voice Business Services:

- ✓ Connected Voice financial information, bank statements, plans and strategies are kept in an electronic folder by the Chief Executive, Head of Business Services, Payroll Manager and Finance Manager. Electronic files containing confidential information about the organisation are password protected and electronic folders have limited access to authorised managers and trustees.
- ✓ Connected Voice bank accounts can only be accessed by authorised members of staff, are password protected and have two factor authentication.
- ✓ Connected Voice Business Services clients' records are kept in confidential electronic folders and are only accessed by the Head of Business Services, Payroll Manager, Finance Manager, Chief Executive and authorised Business Services staff.
- ✓ Client payroll emails or any emails containing personal information are sent by Galaxkey encrypted emails or via Sage payroll system.
- ✓ Clients' records stored on Practice Ignition are password protected.

7. Connected Voice Advocacy – Maintaining Client Data
--

1. Introduction

- ✓ Connected Voice Advocacy is a service delivered by Connected Voice and has specific requirements around confidentiality because of the nature of its work with clients. This section sets out the policies, procedures and guidelines for maintaining client data. This policy is to be used in conjunction with the Data Protection Policy and Mental Capacity Policy, and guidance on non-instructed advocacy approaches.

2. Content

- ✓ Confidentiality is a key principle in the Advocacy Charter and helps to build trust and rapport with people receiving the advocacy service, therefore we ensure people are regularly provided easy-read information on our confidentiality statements and how we store and manage their data.
- ✓ Connected Voice Advocacy holds information of a confidential nature relating to advocates and people needing advocacy.
- ✓ Connected Voice Advocacy works with people in vulnerable situations and who may lack mental capacity to understand and consent therefore we deliver our services in line with the Mental Capacity Act and safeguarding and non-instructed advocacy principles.
- ✓ For this reason, all information held by Connected Voice Advocacy, apart from publicity materials, will be treated as confidential.

3. Recording

- ✓ No information should be recorded unless there is a good reason for it. All workers (paid and unpaid) should be clear why they are making a record before they do so.
- ✓ All workers will take responsibility for explaining to the individual that they are recording information about what is being recorded and why it is being recorded. They should also give a brief statement of our confidentiality policy (for an example see the confidentiality statement below and Confidentiality Client Information Card) and ensure that copies of these procedures, the Connected Voice Confidentiality Policy and the Advocacy Code of Practice are available if requested.
- ✓ All workers will record any decisions taken to withhold information about the person in their Best Interest. Any discussions, research and investigation as well as formal Best Interest processes that take place to reach this decision will be evidenced and documented in the case file.
- ✓ Any decisions to share information with third parties will be documented to demonstrate the process of consent or Best Interest Decision.
- ✓ Any safeguarding procedures relating to the use of/sharing of/recording of data about a person at risk, will be recorded in the case file and Risk Management Strategy.

4. Storage

- ✓ Documents relating to clients are scanned into a secure personal electronic folder and any paper copies are shredded. Access to electronic client folders are restricted to the advocates within the advocacy service. All client folders are saved on the Connected Voice network which is password protected.

- ✓ Advocates may have confidential information at home. If so, such information should be made anonymous wherever possible (removing name and address for example). They should also ensure that this is not available to others.

5. Handling

- ✓ Material should never be left lying about on a desk in an area where members of the public have access.
- ✓ Any messages or confidential papers being passed to another member of staff or volunteer will be done so via email.
- ✓ Staff need to be careful when using confidential material on a VDU screen that it is not visible to unauthorised people.
- ✓ Staff who are working on confidential material, and who go for a break for whatever reason, should ensure that they put away any sensitive material.
- ✓ In the office, any interviews with, or discussions about advocates and/or partners, should take place in one of the interview rooms or private place.

6. Information on Computer

- ✓ The storage of files and letters on computer needs to be considered and appropriate information on the storage given to whoever types the information for you. There are a variety of storage places on the computer depending on the level of security.
- ✓ Client contact details, case notes and statistical information is kept on the Connected Voice Advocacy Cygnet Database. Connected Voice Advocacy staff have access to these details.
- ✓ Connected Voice Advocacy uses the Lamplight database for client records. This is a cloud based database that is password protected and only advocates within the advocacy service has access to the client records and information.
- ✓ All laptops and mobile devices are encrypted.

7. Access to our records

- ✓ Any confidential material which is held on an individual, will be accessible to them unless we owe a prior duty of confidentiality to someone else (e.g. we promise referees that the references they give will be treated in confidence).
- ✓ On occasion we may be given information which we are asked to keep confidential because it is third party information or may risk serious harm. In these circumstances, the issue will be discussed with the Connected Voice Advocacy Manager who will make a judgement on whether it is appropriate for us to withhold this information. This will only be done in exceptional circumstances and, if so, Connected Voice Advocacy will ensure that the

information is clearly identified and separated from all records to which the advocacy partner might request access and the rationale for withholding the information is recorded.

- ✓ Any information will remain confidential within Connected Voice Advocacy and the Chief Executive of Connected Voice. Thus, an advocate will be free to seek support in regard to advocacy issues from their Coordinator, and staff will be free to seek such support from their colleagues/line managers.
- ✓ No information will be given to a third party unless the client expressly agrees that it should be released, or unless we are required by law to do so. When someone lacks the mental capacity to agree to information sharing, advocates will work within the Best Interest Framework with stakeholders, supporting a Best Interest Decision which will be recorded.
- ✓ Where there is a requirement for Connected Voice Advocacy to provide confidential records, e.g. where we are contracted to provide advocacy under a Personal Injury compensation claim, express consent on a Form of Authority will be required from the client if they have capacity to understand and give consent and/or countersigned by an appropriate person acting officially on their behalf (e.g. Litigation Friend, Official Solicitor). This consent must be renewed every 6 months. Third party information will be redacted where appropriate.

8. Access to information in records that would not necessarily be disclosed and withholding information

- ✓ Connected Voice Advocacy may take a considered decision to withhold information from a third party or the person receiving advocacy for risk of harm or distress. This will be recorded as a Best Interest Decision and the Independent Advocate will follow the non-instructed advocacy principles in the Mental Capacity Act Policy.
- ✓ People receiving advocacy and third parties involved in the case will receive information on how we store and manage data. It will be explained that we will only share data with consent. Data will only be shared without consent by the person receiving advocacy when legally required to or if someone involved is at risk of harm.
- ✓ To reinforce the principles of confidentiality we will record and challenge all data breaches into the organisation and remain transparent with the person we advocate for on any data received by or shared by third parties (including Social Workers, Case Managers, Financial Deputies, Interpreters, Advocacy providers etc .
- ✓ To ensure clarity on our position to be alongside the person all Independent Advocate Signatures include the statement '*As advocates we work as an extension of the person we work with, and therefore will share information with them*'.

- ✓ Independent Mental Health Advocates (IMHAs) have a legal right to see relevant records in order to help and support patients. This includes information in records which the patient themselves would have no right to see (because it would not normally be disclosed to the patient under the Data Protection Act either because it is provided by or relates to a third party or because it would risk serious harm to the patient or anyone else). See 'Independent Mental Health Advocates Supplementary guidance on access to patient records under Section 130B of the Mental Health Act 1983': Department of Health.
- ✓ In order to be clear about confidentiality in these circumstances Connected Voice Advocacy will ask for consent from the patient about whether they want the IMHA to have access to all of the patient's relevant records or just those that the patient would have a right to see (see IMHA Access to Records Patient Consent Form).
- ✓ When the IMHA requests access to a patient's records they will identify (on the Access to Records Request Form) whether the patient has consented to the IMHA requesting third party information and information which may cause serious harm. Where the patient lacks capacity to consent, the IMHA will provide Non-Instructed Advocacy within Mental Capacity Act principles and in accordance with the Mental; Capacity Act Policy.
- ✓ On return of the records the IMHA will check to see whether anything has been identified by the record holder which should be withheld from the patient and ensure that this is clearly identified and separated from all records to which the patient might request access.
- ✓ The IMHA must ensure that they do not disclose any of the information identified in 8.4 above to the patient or even tell them that it exists.

9. Confidentiality and Risk

- ✓ Advocates need to be able to stay loyal to the advocacy relationship, and in order to maintain this, Connected Voice Advocacy needs to be as clear as possible about when and how confidentiality might be broken. Where possible, an individual should stay in control of what happens to information about them. Connected Voice Advocacy should only, in exceptional circumstances, share information with an outside organisation or take action without the consent of an Advocacy Partner if:
 - ✓ there is a substantial or imminent risk of harm or danger;
 - ✓ or when not to do so would be breaking the law.
- ✓ Passing on information under these circumstances may be part of carrying out necessary action related to an individual's basic rights and needs. A detailed set of guidelines will be drawn up to deal with this situation.

10. Disposal

- ✓ Once a person has ceased to be an advocate with Connected Voice Advocacy or a partner is no longer receiving support from an advocate, any information will be kept for a period of 7 years. Then if no further contact has occurred, the information will be shredded.

11. Example material

- ✓ We may have occasion to use example material on a number of occasions - giving talks to raise awareness, developing case studies for training, writing evaluation reports, providing case notes for commissioner audits and quality assessments. Whenever this is done due regard must be given to the ownership of the story and the confidentiality of the person concerned. The individual(s) concerned should be approached for permission to use their story and, if permission is given, consideration should be given to making the individual anonymous (e.g. changing name, gender, area where they live etc.).

12. Meetings and Gatherings

- ✓ Staff, and sometimes advocates, can be given information when it is not clear whether it is confidential or not (e.g. referral information). It is important that all workers make sure that they are clear about the status of the information being offered. If it is of a confidential nature, they should be sure that they really need to know the information that is being offered.
- ✓ Information that is held on individuals is available to that person on request.

13. Conclusion

- ✓ These guidelines will not cover every eventuality. Anyone in doubt about an issue of confidentiality should consult the Connected Voice Confidentiality Policy and the Advocacy Code of Practice for guidance on principles, and seek the view of their Coordinator/line manager

14. Connected Voice Advocacy – Confidentiality Statement

In most circumstances any information that you share with your advocate will remain confidential to Connected Voice Advocacy.

The advocate will not disclose any information about you to another person or agency without your permission unless you or another person is at risk of harm or we are legally required to do so. If you lack the mental capacity to decide for yourself, we will make sure your views, wishes and beliefs are considered.

If you are unhappy about the service you are receiving and are unable to resolve this with the advocate, please contact the Advocacy Coordinator or the Connected Voice Advocacy Manager.

This is taken from the Advocacy Code of Practice which all our advocates must work to. If you would like a full copy of the Code of Practice please contact Connected Voice Advocacy.

15. Guidelines on Breaching Confidentiality

- ✓ Connected Voice Advocacy will keep information confidential within the Centre and the Chief Executive of Connected Voice. Thus, an advocate will be free to seek support with regard to advocacy issues from their Co-ordinator, and staff will be free to seek such support from their colleagues/line managers.
- ✓ A log will be kept of any breaches of confidentiality (including accidental breaches), including action taken and learning points [kept in Confidential drive Avocfd\Confidentiality\Log of breaches of confidentiality].

16. Breaching confidentiality where there is risk of harm or abuse

The only exception to this rule is in circumstances of significant danger including abuse where the following guidelines will apply:

- ✓ In the event of an allegation of abuse or other risk to the service user or to others, the advocate should accept what is being said and deal with the situation immediately.
- ✓ The nature, circumstances and seriousness should be determined.
- ✓ The advocate should make every attempt to contact their line manager or Advocacy Coordinator to discuss the situation within one working day. The line manager or Coordinator will offer support and guidance seeking further clarification through line management if necessary.
- ✓ If the line manager, Coordinator or Connected Voice Advocacy Manager is not available and the advocate considers that the service user is in imminent danger, for example through abuse that is life threatening, the matter should be reported without delay to the appropriate authority (e.g. Police or Social Services emergency duty team). This should happen even if the service user does not give consent.
- ✓ Attempts should be made to gain the confidence of the service user and obtain permission to contact other agencies. Remember there is no breach of confidentiality if permission to disclose to others is given.
- ✓ If the matter is less urgent and can wait until a line manager or Coordinator can be contacted, a judgement will then need to be reached together as to whether to:
 - inform the Social Services Department or other appropriate person or organisation, without the service user's consent
 - continue for a fixed period of time to support and persuade the service user to report the situation themselves with our support if they wish

- respect the wishes of the service user and explain the consequences of not reporting the situation

Factors involved in this judgement will be:

- Is there any risk to a third party?
 - Is there a child involved?
 - The level of understanding and communication of the service user
 - The seriousness, circumstances and nature of the abuse
 - The timing of the abuse: did it happen some time ago; recently or is still happening or likely to happen again?
 - Breaking the trust placed in the advocate by the service user may lead to withdrawal of and denial of the disclosure.
- ✓ In the event that any allegation of abuse or other disclosure involves a child or young person or there is a risk to a third party, the matter will be reported without delay to the relevant authority.
 - ✓ The Advocate and line manager/Coordinator should be offered a debriefing session in addition to the ongoing support they receive.
 - ✓ A careful record needs to be kept of both the events leading up to a possible breach of confidentiality, and discussions which lead to making any decisions and/or taking action as above.
 - ✓ It is important to note that at any time Connected Voice Advocacy may be held accountable for the actions of both staff and volunteers involved with the organisation, and this should be balanced with the primary concern of the welfare of the service user.
 - ✓ Any person using Connected Voice Advocacy should be made aware of this policy at an early stage of their involvement with the organisation. Every effort should be made to explain the policy to service users, and a variety of communication aids should be used, if necessary, to enable a service user to understand the policy to a level their skills allow. If a person has enduring Mental Health Problems and is likely to pose a risk, an advance statement could be drawn up with the partner outlining how they would like the situation to be dealt with within the confines of this policy.
 - ✓ Staff and advocates need to be aware of the sensitive nature of the policy, and ensure that any service user understands why a breach of confidentiality may need to take place.
 - ✓ The service user will need to remain confident that only in extreme circumstances will information be shared with any person outside of the organisation, so as not to inhibit the development and trust in an advocacy partnership.

17. Accidental breaches of confidentiality

- ✓ Connected Voice Advocacy and Connected Voice take all reasonable measures to ensure accidental breaches of confidentiality do not occur. If an accidental breach does occur, the following guidelines and procedure will apply:
- ✓ In the event of an accidental breach of confidentiality or an allegation that confidentiality has been breached inadvertently, the situation should be dealt with immediately
- ✓ Where an advocate is involved, they should make every attempt to contact their line manager or Advocacy Coordinator to discuss the situation within one working day. The line manager or Coordinator will offer support and guidance seeking further clarification through line management if necessary.
- ✓ If the line manager, Coordinator or Connected Voice Advocacy Manager is not available and the advocate considers that the service user is in imminent danger, for example through abuse that is life threatening, the matter should be reported without delay to the appropriate authority (e.g. Police or Social Services emergency duty team). This should happen even if the service user does not give consent.
- ✓ The nature, circumstances and seriousness should be determined.
- ✓ Any risk to service users or others should be assessed immediately and action taken as appropriate.
- ✓ Immediate action should be taken to minimise any risk.
- ✓ Any staff or volunteers involved should be offered a debriefing session in addition to the ongoing support they receive.
- ✓ A careful record needs to be kept of both the events leading up to an accidental breach of confidentiality, and discussions which lead to making any decisions and/or taking action as above. A detailed record should be kept of any actions taken and learning points. Any policy or practice issues will be taken to the relevant forum (e.g. Advocacy Team Meeting, Management Group, Trustees).
- ✓ Any breaches will be reported as appropriate and in adherence with the Connected Voice Data Protection policy (e.g. to the Information Commissioner's Office)
- ✓ It is important to note that at any time Connected Voice Advocacy may be held accountable for the actions of both staff and volunteers involved with the organisation, and this should be balanced with the primary concern of the welfare of the service user.

For instances of abuse staff should refer to the Connected Voice Safeguarding Policies and Procedures.

8. Processing confidential information

Confidential information is at its most vulnerable when it is going through the administration system. Care should be taken when processing confidential information as follows:

- ✓ Confidential information should not be left uncovered on a desk when leaving the workstation
- ✓ Confidential information should not be left displayed on a computer screen when leaving the workstation
- ✓ Confidential information being handed to an administrator should always be concealed in a file or envelope marked “Confidential”
- ✓ Administrators working in the public areas of Connected Voice office should be particularly careful about leaving confidential information on display

9. Limits to client confidentiality

In some circumstances Connected Voice reserves the right to break confidentiality should this be deemed necessary. These circumstances include:

- ✓ If a member of staff believes that a client could cause danger to themselves or to others
- ✓ If a member of staff suspects abuse or has knowledge of abuse
- ✓ If the client gives information which indicates that a crime has been committed
- ✓ If disclosure is required by law, for example, by the police
- ✓ If a person is felt to lack the mental capacity to make a decision. In such cases staff or volunteers will discuss with their line manager and they will only act in the client's best interest
- ✓ If the client gives information which indicates criminal activity such as a possible terrorist threat, drug trafficking, money laundering, sexual exploitation or modern slavery

The Connected Voice policies and procedures listed in Section 14 (including the Safeguarding Adults Policy and Safeguarding Children and Young People Policy and Procedure) should be consulted when making decisions about client confidentiality.

The decision on whether to break confidentiality will be decided on a case by case basis and always in conjunction with a line manager.

10. Access to data

This Confidentiality Policy operates on a “need to know” basis and apart from staff, volunteers and trustees in the office of Connected Voice, no-one will have access to client or organisational information unless it is relevant to the service of their work.

All clients have the right to request access to all information stored about them, and have a right to see a copy of this Confidentiality Policy on request.

If any party concerned has a sensory or physical impairment, efforts should be made to ensure that all aspects of this Confidentiality Policy and exchanges between parties are understood. This Confidentiality Policy will be administered in line with the Connected Voice Equity, Diversity and Inclusion Policy.

Significant breaches of the Confidentiality Policy will be dealt with in line with Connected Voice’s Disciplinary Policy and Procedure.

11. Disposal of confidential information

Care will be taken to dispose of confidential information by:

- ✓ Using an onsite shredding company to dispose of confidential information
- ✓ Never placing confidential information in a bin or refuse site
- ✓ Keeping confidential information in as few places as possible and disposing of it in line with the Connected Voice Data Protection Policy and Information Governance Policy on retention of information
- ✓ Staff, volunteers and trustees are informed at their induction about the safe disposal of confidential information. Trustees and volunteers who are working away from the office are instructed to bring confidential documents into the Connected Voice office for safe destruction.
- ✓ Connected Voice uses One Drive for the sharing of board papers to avoid them being saved in multiple places on several computers.
- ✓ Regularly housekeeping electronic files in line with the Connected Voice Data Protection and Information Governance Policy

12. Use of client information for publicity, reporting or training purposes

Connected Voice on occasions may need to be able to give information where appropriate about the impact of its services. If this information is used for publicity, reporting or training purposes, then wherever possible the permission of the client will be sought in writing. If permission cannot be obtained then any details that would enable identification of the client will be changed.

On some occasions examples are used in training events or speeches. While this is a legitimate practice, care will be taken that potentially sensitive material is not used in a way that allows organisations to be identified.

13. Equity, Diversity and Inclusion

All aspects of the Confidentiality Policy will be administered in conjunction with the Connected Voice Equity, Diversity and Inclusion Policy.

14. Meetings and gatherings

Connected Voice staff often facilitate and attend meetings, networks and forums. Organisations that attend these meetings may discuss issues that are confidential. It is important that participants make it explicit the status of the information they are discussing and whether or not it is confidential.

15. Training, evaluation and monitoring

All staff, volunteers and trustees will be given a copy of the Confidentiality Policy when they join Connected Voice. It is the responsibility of all line managers to plan for the appropriate confidentiality systems in their work. Connected Voice will ensure that all staff, volunteers and trustees are trained in the application of this policy and that confidentiality is discussed and monitored in supervision and appraisals. All staff and volunteers must sign a statement to confirm that they have read and understood the Confidentiality Policy and this is kept in their personnel file.

16. Related Connected Voice Policies

This Confidentiality Policy will be administered in line and in conjunction with:

- ✓ Data Protection and Information Governance Policy
- ✓ Safeguarding Adults Policy
- ✓ Safeguarding Children and Young People Policy
- ✓ Equity, Diversity and Inclusion Policy
- ✓ Flexible and Hybrid Working Policy
- ✓ ICT Policies and Procedures
- ✓ Whistleblowing Policy
- ✓ Code of Conduct
- ✓ Supervision, learning and development Policy
- ✓ All legislative