Connected Voice
Data Protection Policy

(Incorporating 2018 General Data Protection Regulations and NHS England Information Governance requirements)

Contents

Document details and review

Organisation	Connected Voice
Responsible person	Lisa Goodwin
Date released	January 2011

This policy will be reviewed annually

Date of last review	Date approved by Trustees	Date of next review
May 2023	13 June 2023	May 2024

Signed by responsible person:
Date: 13 June 2023

1. Scope of the policy

This policy applies to paid staff, trustees and volunteers.

2. Introduction

Purpose of policy
The purpose of this policy is to enable Connected Voice to:
- ✓ comply with the law in respect of the data it holds about individuals
- ✓ follow best practice
- ✓ protect Connected Voice's supporters, staff and other individuals
- ✓ protect the organisation from the consequences of a breach of its responsibilities
- ✓ cover NHS Information Governance contractual requirements

Brief introduction to General Data Protection Regulations 2018
The General Data Protection Regulations 2018 regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Data protection principles
Data users must comply with the data protection principles of good practice which underpin the General Data Protection Regulations and best practice for Information Governance and Data Security and Protection.

Personal data must be:
- ✓ obtained and processed fairly and lawfully
- ✓ held only for specified purpose
- ✓ adequate, relevant and not excessive
- ✓ accurate and up to date
- ✓ not kept longer than necessary
- ✓ processed in accordance with the Regulations
- ✓ kept secure and protected
- ✓ not transferred to countries without adequate data protection

Types of information covered by this policy
Connected Voice holds three types of information:
- ✓ Organisational information – publicly available information about organisations and some confidential information
- ✓ Personal information – information held about individuals such as names, addresses, job titles
- ✓ Sensitive personal information – information held about employees such as health and disability; and service-users such as information about health and disability, safeguarding procedures etc.

Information about organisations is not covered by the General Data Protection Regulations. However, there is sometimes ambiguity about whether certain

information is personal or organisational, for example the contact details for a developing organisation might be someone's home address or personal email address. As Connected Voice strives for best practice, organisational information is covered by this policy.

Personal data
This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the General Data Protection Regulations, by virtue of not meeting the strict definition of "data" in the Regulations.

Key risks
Connected Voice has identified the following potential key risks, which this policy is designed to address:
- ✓ breach of confidentiality (information being given out inappropriately)
- ✓ insufficient clarity about the range of uses to which data will be put – leading to Data Subjects being insufficiently informed
- ✓ failure to offer choice about data use when appropriate
- ✓ breach of security by allowing unauthorised access
- ✓ failure to establish efficient systems of managing changes to our staff and volunteers, leading to personal data being not up to date
- ✓ harm to individuals if personal data is not up to date
- ✓ insufficient clarity and failure to offer choice about how personal data of staff and volunteers and others is used
- ✓ data protection issues in partnerships and other collaborative relationships
- ✓ data protection issues in relation to contractors and other external bodies
- ✓ data processor contracts

3. Policy statement

Connected Voice will:
- ✓ comply with both the law and best practice
- ✓ respect individuals' rights
- ✓ be open and honest with individuals whose data is held
- ✓ provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently
- ✓ *complete NHS England Data Security and Protection Toolkit on an annual basis. Completed April 2023*

Connected Voice recognises that its first priority under the General Data Protection Regulations is to avoid causing harm to individuals. In the main this means:
- ✓ keeping information securely in the right hands, and
- ✓ holding good quality information

Secondly, the Regulations aim to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Connected Voice will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

4. Responsibilities

Trustees
The board of trustees recognises its overall responsibility for ensuring that Connected Voice complies with its legal obligations.

Data Protection Officer
The Data Protection Officer is currently the Chief Executive, with the following responsibilities:

- ✓ briefing the board on data protection responsibilities
- ✓ reviewing data protection and related policies
- ✓ advising other staff on data protection issues
- ✓ ensuring that data protection induction and training takes place
- ✓ reporting data breaches to the Information Commissioners Office
- ✓ handling subject access requests
- ✓ approving unusual or controversial disclosures of personal data
- ✓ approving contracts with data processors

Connected Voice Core Support
The Connected Voice Core Support Team is responsible for managing the ICT network and keeping it secure.

Team/department/managers
Each team or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training) to ensure that good data protection and information governance practice is established and followed.

For each new project, managers are responsible for systemically identifying and minimising the data protection risks. For each new project managers should complete Appendix 7: Retention Periods and Subject Access Rights, unless the project falls within an area already defined in the table.

Staff and volunteers
All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal and organisational data they may handle in the course of their work.

Enforcement
Significant breaches of this policy will be handled under the Connected Voice disciplinary procedures.

5. Confidentiality

Scope
Because confidentiality applies to a much wider range of information than data protection and information governance, Connected Voice has a separate confidentiality policy.

Communication with Data Subjects
Connected Voice will have a privacy statement for Data Subjects, setting out how their information will be used. This will be available on request, and a version of the statement will also be used on the Connected Voice website. (See appendix one)

Communication with staff
Staff, trustees and volunteers will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See appendix two)

Authorisation for disclosures not directly related to the reason why data is held
Where anyone within Connected Voice feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Officer. Connected Voice Advocacy and other Connected Voice services must consult their own confidentiality policy and procedures in conjunction with this Data Protection Policy. All such disclosures will be documented.

6. Security

Scope
This section of the policy only addresses security issues relating to personal data.

Specific risks
Connected Voice has identified the following risks:
- ✓ protecting data while it is in transit
- ✓ staff or volunteers with access to personal information could misuse it
- ✓ poor web site security might give a means of access to information about individuals once individual details are made accessible on line
- ✓ staff may be tricked into giving away information, either about supporters or colleagues, especially over the phone
- ✓ unauthorised access by staff and volunteers while working and no longer working for Connected Voice

Security measures
- ✓ If in transit with sensitive and confidential paper records staff must:
    - Make sure that there is no option available to them
    - Never take the only copy with them if it is practical to make and retain a duplicate or copied on the system. Staff must assess the impact of loss of the original and make a copy if that impact is unacceptable
    - Take only as much as necessary and only for as long as necessary
    - Transfer it back to its normally secure location as soon as possible
    - Take all reasonable precautions to keep records safe and secure
- ✓ Access to data, information and files is defined by job role, and controlled through passwords
- ✓ All voice over the internet phones are password protected
- ✓ All memory sticks are encrypted and only used for presentations
- ✓ All mobile phones used for work purposes are password protected

- ✓ All computer systems containing personal data have individual logins
- ✓ All firewall hardware and software are kept up to date to protect servers from hackers
- ✓ Training is provided on database use to reinforce confidentiality and data protection
- ✓ All passwords for networking components, such as Wi-Fi, are changed from their original passwords
- ✓ Pasportal is used to store passwords safety and stores appropriate access to levels for staff members
- ✓ All staff to complete Level 1 Data Security Awareness training on an annual basis and the Data Protection Officer to complete advanced Data Security training

Back up
Data, information and files are regularly and securely backed up following the backup policy.

Software updates
The latest software updates are downloaded and installed by the Connected Voice external ICT support provider. This ensures all IT systems and devices have the latest and appropriate software and application updates.

Sending and receiving confidential information by email
Care will be taken when sending confidential information by email to ensure its security. Confidential information will only be sent by email if a recipient name and email address has clearly been identified as secure and a system is in place for ensuring that the correct recipient receives the email. Systems are in place to ensure that emails containing confidential information received by us are identified and stored in a secure place.

To ensure emails are secure all firewall hardware and software are to be kept up to date to protect servers from external attacks. For additional security, staff have the option of using Galaxkey encrypted emails, which is available to all staff. Advocates have access to and must use an NHS email address to send and receive confidential or client identifiable data to third parties.

7. Data recording and storage

Accuracy
Connected Voice holds data in several organisation and project specific databases, and record and storage systems. To help us deliver our activities and manage the organisation.

Connected Voice will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:
- ✓ ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data

- ✓ Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets
- ✓ Effective procedures will be in place so that all relevant systems are updated when information about any individual changes
- ✓ Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping

Updating
Connected Voice regularly house keeps and reviews the data kept.

Retention periods
Connected Voice will establish retention periods for at least the following categories of data:

- ✓ Connected Voice member organisations
- ✓ Connected Voice users of services
- ✓ Connected Voice supporters
- ✓ Connected Voice Advocacy clients
- ✓ Connected Voice DIY Advocate users
- ✓ Connected Voice volunteers, across all teams
- ✓ Staff
- ✓ Connected Voice trustees
- ✓ OurGateshead website groups and organisations

See Appendix Seven for retention periods for each Connected Voice team.

Archiving
Archived paper records of data subjects are stored securely in locked filing cabinets. Archived electronic records of data subjects are stored securely in restricted and confidential electronic folders.

Connected Voice Advocacy's case management database has an archiving and anonymisation facility which enables us to completely anonymise client records after retention periods (according to contracts and data protection guidance), leaving only basic anonymous information for monitoring and reporting purposes e.g. client numbers within each service.

Disposal
Records of data subjects will be securely shredded once they have reached the end of the retention period.

8. Data breach

Scope
This section of the policy only addresses issues relating to a personal data breach.

Guidelines
It is mandatory to report a personal data breach to the Information Commissioners Office under the General Data Protection Regulations if it is likely to result in a risk to

people's rights and freedoms. The thresholds to determine whether an incident needs to be reported depends on the risk it poses to people involved. In this section, we define an example low-level data breach, which does not need reporting to the Information Commissioners Office, and an example of a high-level data breach, which does need reporting to the Information Commissioners Office.

Incidents that Connected Voice may face that constitute a data breach:

- ✓ Staff or volunteers losing data in transit
- ✓ Staff or volunteers with access to personal information misusing it
- ✓ Staff tricked into giving away information, either about supporters or colleagues, especially over the phone
- ✓ Staff or volunteers accidently sending personal information to the wrong person, especially by email
- ✓ Connected Voice servers hacked and personal information falling it other people's hands or made accessible on line
- ✓ Unauthorised access by staff and volunteers while working and no longer working for Connected Voice

A data breach has a potential of people and Connected Voice suffering significant detrimental effect, for example, discrimination, damage to reputation, financial loss, or any other significant economic and social disadvantage.

Process for a low-level data breach

Example of a low-level data breach is when you accidently send client data to the wrong recipient who is another professional and they delete it. If you are unsure, please consultant you line manager. Process:

1. You should notify your line manager of the data breach and add it to the Data Breach Log stored in the Common Drive\GDPR\Data Breach Log
2. At the year end the Data Breach Log is reported to the Information Commissioners Office

Process for a high-level data breach

Example of a high-level data breach is when hackers obtain client information, which results in a risk to their personal rights and freedoms. If you are unsure, please consultant you line manager. Process:

1. You should report a data breach immediately to your line manager
2. Line manager to inform Data Protection Officer
3. The Data Protection Officer should inform the Information Commissioners Office within 72 hours of Connected Voice becoming aware of the data breach even if they are not aware of all the details at this stage
4. Reporting needs to be open and honest without undue delay – tell it all, tell it fast, tell the truth

Data breach by another organisation

Where Connected Voice staff experience a data breach by another organisation they have a professional courtesy to inform the organisation that they have breached personal data.

9. Subject access

Responsibility
Any data subject requests will be handled by the Data Protection Officer and dealt with within one month of the first date of the request being received by Connected Voice. The first date of request will be recorded on the Subject Access Request Log saved in Common/GDPR/Subject Access Request Log.

Procedure for making a Subject Access Request
When an initial enquiry is received a Subject Access Request form will be sent out immediately and the date it is sent out and received back will be recorded on the Subject Access Request log. The Subject Access Request Form can be found in Appendix 3 of this policy.

All staff and volunteers are required to pass on to their line manager/supervisor anything which might be a subject access request.

All those making a subject access request will be asked to identify anyone else who may also hold information about them, so that this data can be retrieved.

Provision for verifying identity
Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

Charging
We will provide information free of charge.

However, we will charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. We will also charge a reasonable fee to comply with requests for further copies of the same information.

Procedure for granting access
The required information will be provided in permanent form by letter or email unless the applicant makes a specific request to be given supervised access in person.

See Appendix Seven for subject access rights for each Connected Voice section

Procedure for dealing with a complaint
Where an individual makes a complaint to Connected Voice relating to our use and processing of their data or a relative's data, you are to inform the Data Protection Officer immediately. The Data Protection Officer, working with the service manager, will investigate and respond to the complaint as soon as possible. The Data Protection Officer is to inform the Board immediately of the details of the complaint and proposed actions.

10. Transparency

Commitment
Connected Voice is committed to ensuring that in principle Data Subjects are aware that their data is being processed and:

- ✓ For what purpose it is being processed
- ✓ What types of disclosure are likely
- ✓ How long we will hold the information
- ✓ How to exercise their rights in relation to the data

Procedure
Data Subjects will generally be informed in the following ways:

- ✓ Staff: in the staff handbook
- ✓ Volunteers: in the volunteer support pack
- ✓ Connected Voice members: in the welcome letter and information
- ✓ Connected Voice supporters and users of services: when they sign up (on paper, on line or by phone) for services or purchase products
- ✓ Data Privacy Notices for service areas
- ✓ Connected Voice Advocacy clients: in data protection statement (e.g. on referral/consent form, client confidentiality card)

Data Privacy Notices will be provided to staff for use where data is collected (see appendix four).

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

11. Consent

Underlying principles
Consent will normally not be sought for most processing of information about staff, with the following exceptions:

- ✓ Staff details will only be disclosed for purposes unrelated to their work for Connected Voice (e.g. financial references) with their consent
- ✓ Staff working from home, will be given the choice over which contact details are to be made public

Information about volunteers will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

Information about members and service users will only be made public with their consent. (This includes photographs). When clients lack the 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.

"Sensitive" data about members and service users (including health information) will be held only with the knowledge and consent of the individual.

Forms of consent
Consent will be written with the data subject signing to confirm Connected Voice can process their data. For referrals made on behalf of people lacking capacity, a signature is not required as the referral is made in the person's best interest.

Opting in
A person has to opt in for Connected Voice to use their data. If a person does not opt in Connected Voice cannot use their data.

Withdrawing consent
The organisation acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Right to be forgotten
Also referred to as 'the right to erasure'. A person can make a request verbally or in writing to Connected Voice for their personal data to be erased. This right only applies to data held at the time of the request is received and must be responded to within one month of the request. The right is not absolute and only applies in the following circumstances:

- ✓ the personal data is no longer necessary for the purpose which you originally collected or processed it for
- ✓ you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent
- ✓ you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- ✓ you are processing the personal data for direct marketing purposes and the individual objects to that processing
- ✓ you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle)
- ✓ you have to do it to comply with a legal obligation; or
- ✓ you have processed the personal data to offer information

12. Direct marketing

Underlying principles
Connected Voice will treat the following direct communication with individuals as marketing:

- ✓ Seeking donations and other financial support
- ✓ Promoting any Connected Voice services
- ✓ Promoting events
- ✓ Promoting membership to supporters

- ✓ Promoting sponsored events and other fundraising exercises
- ✓ Marketing the products of
- ✓ Business Services Ltd
- ✓ Marketing on behalf of any other external company or voluntary organisation

Opting out
Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all Connected Voice marketing.

Sharing lists
Connected Voice has the policy of sharing lists (or carrying out joint or reciprocal mailings) only on an occasional and tightly-controlled basis. Details will only be used for any of these purposes where the data subject has been informed of this possibility, along with an option to opt out, and has not exercised this option.

Connected Voice Advocacy does not share lists.

Electronic contact
Connected Voice will only carry out telephone or email marketing where consent has been given in advance. Our membership and other forms check whether data subjects are happy to be contacted by email or telephone.

Whenever email addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

13. Staff training and acceptance of responsibilities

Documentation
Information about data protection for staff is contained in the staff handbook.

Other related policies
This policy should also be read in conjunction with:
- ✓ Confidentiality policy
- ✓ Whistleblowing policy
- ✓ ICT in Connected Voice handbook
- ✓ Recruitment and selection guidelines and systems
- ✓ Mental Capacity policy

Induction
All staff who have access to any kind of personal data will have their responsibilities in relation to data protection and information governance outlined during their induction procedures.

Data protection and information governance will be included in training for volunteers and staff.

Continuing training
Connected Voice will provide opportunities for staff to explore data protection issues through training, team meetings and supervisions.

It is mandatory for all Connected Voice staff and trustees to annually complete Data Security Training and record this training on Breathe.

At all Connected Voice Full Staff meetings cyber security is a standing item on the agenda.

Data Security Training and other mandatory training features on the supervision form to allow managers to check that staff have completed on an annual basis.

Procedure for staff signifying acceptance of policy
Connected Voice staff, volunteers and trustees will be required to sign a form during their induction period to confirm they have read and understood the Data Protection Policy, including information governance.

3. Definitions of terms

Data
Information held on computer or, in many case, on paper (including photographs, video material).

Data Controller
The Data Controller is the legal person or organisation responsible for complying with the General Data Protection Regulations ie responsible for how and why personal data is used.

Data Processor
An organisation or individual to whom data processing has been outsourced. When work is outsourced, which involves the contracting organisation in having access to personal data; there must be a suitable written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of data protection brought about by the Data Processor.

Data Subject
An individual about whom personal data is held.

Data Privacy Notice
Information for a Data Subject telling them in a clear and transparent way the legal basis for the Data Controller to hold their data, how we will use the data and how long the data will be held.

Direct marketing
The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

Personal data

Information about a living individual who is identifiable from the data held on them by a Data Controller.

Processing
Any use of personal data, including obtaining, storing, using, disclosing or destroying.

Record
A set of information about one individual.

Subject access
The right of an individual to have a copy of the information a Data Controller holds about them.

Third party
This refers either to the fact that the data is about someone else other than the Data Subject or someone other than the Data Subject is the source.

Appendix one – privacy statement

When you request information from Connected Voice, sign up to any of our services or buy things from us, Connected Voice obtains information about you. This statement explains how we look after that information and what we do with it.

We have a legal duty under the General Data Protection Regulations and NHS Information Governance requirements to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally the only information we hold comes from you or that held in the public domain. Whenever we collect information from you, we will make it clear which information is required in order to provide you with the information, service or goods you need. You do not have to provide us with any additional information unless you choose to. We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

Communications and marketing
We would also like to contact you in future to tell you about other services we provide, and ways in which you might like to support Connected Voice. You have the right to ask us not to contact you in this way. We will always aim to provide a clear method for you to opt out. You can also contact us directly at any time to tell us not to send you any future marketing material.

Very occasionally we carry out a joint mailing with carefully selected other organisations to tell you about products and services we think you might be interested in. Again, you have the right to opt out of this.

Accessing your data
You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy, either ask for an application form to be sent to you, or write to the Data Protection Officer at Connected Voice. We aim to reply as promptly as we can and, in any case, within one month of the request.

Our website and data
For the Connected Voice website and OurGateshead website, Connected Voice uses Google Analytics to monitor usage.

The Connected Voice website does not automatically capture or store personal information, other than logging a user's IP address and session information such as the duration of the visit, type of browser and pages visited. This information may be processed to enable anonymous analysis of the usage of the site to aid site development. In the event of a breach of security it may also be used to aid detection.

The OurGateshead website, allows users to create account and upload information about the group or organisations they have involvement in. Upon doing this, you will be given an encrypted password, which no one in Connected Voice or outside the organisation has access to. Connected Voice runs OurGateshead on behalf of Gateshead Council.

If you use any of the online enquiry forms to request further information from Connected Voice, information entered will be emailed to Connected Voice and recorded in our database. Your contact details will be used to respond to your enquiry and the nature of the enquiry included anonymously in statistical reports to funders and other stakeholders. All personal information supplied will be held securely in accordance with GDPR and we will seek your express permission before using it for any other purpose.

Connected Voice Advocacy
Because of the requirements of the General Data Protection Regulations, a signature is needed to say that you agree to Connected Voice Advocacy securely holding personal information (including the information on this form), on a secure electronic case management system, a computer and in a paper filing system. It is the policy of Connected Voice Advocacy that all personal data will be held in accordance with the principles and requirements of General Data Protection Regulations other relevant legislation and that procedures will be put in place to ensure the fair processing of data relating to individuals. Connected Voice Advocacy is a confidential service. You can request further information on confidentiality from us.

Appendix two – confidentiality statement for staff and volunteers

When working for Connected Voice, you will often need to have access to confidential information which may include, for example:

- ✓ Personal information about individuals who are members, users of our services or otherwise involved in the activities organised by Connected Voice
- ✓ Information about the internal business of Connected Voice
- ✓ Personal information about colleagues working for Connected Voice

Connected Voice is committed to keeping this information confidential to protect people and Connected Voice itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the General Data Protection Regulations, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by Connected Voice to be made public, for example on the online database. Passing information between Connected Voice and a mailing house, or vice versa does not count as making it public, but passing information to another organisation does count. You can share information about organisations where this information is already in the public realm, for example registered charities, but you should still be careful about information that can be linked to individuals (staff, volunteers, trustees and users) connected with organisations. This is also in line with the Information Governance requirements of the NHS.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- ✓ Not compromise or seek to evade security measures (including computer passwords)
- ✓ Be particularly careful when sending information outside the office
- ✓ Not gossip about confidential information, either with colleagues or people outside Connected Voice
- ✓ Not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for Connected Voice.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.

Signed: Date:

Appendix three – GDPR subject access request form

Connected Voice use
Date received
Date completed
Connected Voice

Connected Voice
General Data Protection Regulation subject access request form

Subject access request (2018 General Data Protection Regulation)

You are entitled to see most of the information we hold about you. If you want to see it, please fill in this form and hand it in to the office.

Your name

Your address

Postcode

Telephone number (if you wish)

Email address (if you wish)

Please tick if you have ever been

☐ an employee ☐ a volunteer ☐ a client/used our services

If you have not ticked any of the above, please tell us of any reason why you think we might have information about you

If we may have known you under a different name, please tell us here

If you are only interested in particular information, please say what it is

I want to see the records you hold on me.

Signed Date

Please note

- ✓ If the address you give above does not match the one in our records, we may have to ask you for additional identification.
- ✓ If you are not the data subject (the person the information is about), we will need evidence that you are authorised to act for the subject.
- ✓ We will reply within one month of receipt. If you have asked for a copy of the information, we will send it to the address you have given above.
- ✓ We have information about members of our organisation, staff, volunteers, clients and people we think might be interested in our work. We do not keep this information once we no longer need it, so if you were in touch with us sometime ago we may no longer have any information about you.
- ✓ We will provide everything we have about you, except that we may be allowed to hold back information which is also about, or which identifies someone else.

Appendix four – data privacy notices

When requesting personal data from a Data Subject (staff, trustee, volunteer, service user, client, group or organisation) all staff are to provide the individual with a Data Privacy Notice.

The Data Privacy Notice outlines the legal basis for the Data Controller to hold their data, how the data will be used and how long the data will be held.

Data Privacy Notices exist for:

- ✓ Connected Voice Advocacy – For Connected Voice Advocacy clients.
- ✓ Connected Voice DIY Advocate – For Connected Voice DIY Advocate users.
- ✓ Central Team – For job applicants.
- ✓ Central Team – For Connected Voice staff, trustees and volunteers.
- ✓ Connected Voice Haref – For organisations who want to become members of Connected Voice Haref.
- ✓ Connected Voice Support and Development Team – For organisations who want to become members of Connected Voice.

Appendix five - Information Commissioner's Office: Subject Access Request checklist

Click on the image below to access checklist:

Appendix six – Redacting documents procedure

Compliance

Most redacting is necessary for internal purposes e.g. monitoring or case studies. However we are often called upon to share documents with third parties usually for audits or evidence in court hearings. Before doing so we must follow Connected Voice Data Protection Policy and ensure the party requesting data has officially requested via SAR, Court Order or existing contract clause permissions.

Charges

We will provide information free of charge. However, we will charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. We will also charge a reasonable fee to comply with requests for further copies of the same information.

How to redact

Consider which documents are required e.g. Case notes from cygnet, case studies, external letters and forms, statutory reports. Remove all reference to:

- Identifiable data from or about third parties
- Identifiable date from or about client – where SAR is from a third party

- Replace the above with xxxx or replace the name with profession e.g. replace "John Smith" with "Solicitor" or "Advocate" or "Social Worker"
- Remove or amend any obviously identifiable data e.g. "45 year old polish woman from Durham involved in high profile St Aiden's care home abuse scandal in 2018". Eg "~~45~~ year old ~~polish~~ woman from ~~Durham~~ involved in high profile ~~St Aiden's care home~~ abuse scandal in ~~2018~~".

Tips

- For electronic copies - Use Word to delete, fill in or replace the chosen words and phrases.
    - Replace using the "find and replace" option and type the word you wish to remove and select a replacement word across the whole document
    - Fill – use the highlighter icon and select a black text line filler as this shows something was there before it was filled in
- When using the "find and replace" tool on word be sure to include any variations or abbreviations. Do not rely solely on this function due to typos and entry errors.
- For hard copies - Block out with black ink pen or tippex on paper versions, then photocopy all pages individually to ensure no trace of original information can be seen, test visibility holding document to the light/window
- Print non-word documents such as certificates and letters and physically blocking out the confidential data with ink or Tippex and photocopying or rescanning in client's folder
- Cygnet – click on image of a printer. This provides a print preview. This produces a document of case notes. Click on the Excel to Word icon on the top address bar. Then save the document somewhere secure that you can access. Now you have all your client records in a word document to amend

- A full read of the document is necessary to ensure notes are non-identifiable, any all abbreviations and typos have been anonmyised.

Appendix seven – Retention periods and subject access rights

Data protection audit and retention table – February 2022

This table is to be used to check what personal data we collect at Connected Voice, who we collect it from, what we do with it and what consent we get. The data protection act says that 'data subjects' are individuals however at Connected Voice we work with individuals and organisations. We need to know what information we collect about all these groups and what we do with it. This is partly because we tend to treat organisations in the same way as individuals and it is unclear how unincorporated associations are treated under the data protection act.

This audit will gather information for the retention and subject access table, an appendix of the data protection policy.

Please scroll to the right to ensure all columns are filled in. Add more rows as needed for your work.

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
Connected Voice (Supporting and Developing)	Organisations and individuals	Organisation contact details, individual contact details, email addresses	Connected Voice e-inform, Connected Voice Haref bulletin, On the Hoof email, distribution and Inform distribution	Lamplight	All staff with Lamplight accounts includes password access	Unsubscribe info clearly stated in email and hard bounce backs dealt with weekly	As long as subscribed	We use it to manage their subscription and it isn't shared	Individuals contact details i.e. those who are members of the general public and not part of an organisation are covered by the General Data Protection Regulations	Information stored on Lamplight which is password protected. Only Connected Voice staff and volunteers can access this information	Information stored in electronic files on Connected Voice computers All computers are password protected Only Connected Voice staff & volunteers can access this	Paper files will be kept in a locked filing cabinet for one year and then destroyed

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
											information	
Connected Voice (Chief Executive and Office Manager)	Organisations	Organisation contact details (addresses, staff, info in public domain)	Membership	Lamplight	All staff with Lamplight accounts includes password access	Updated on an biannual basis to ensure information held is correct	As long as they are members of Connected Voice	We tell members that their information will be kept on a central database	No – information is in the public domain, so no legal right to access data	N/A	N/A	N/A
Connected Voice (Chief Executive, Line Manager and Office Manager)	Staff	Staff contact details, email addresses, telephone numbers, home addresses Payroll data Right to work Induction data Flexiplanners Health and medical data Ethnic monitoring data Disciplinary and grievance records Supervision notes/appraisals Pension data	Staff records	Paper and IT – done this for Business Continuity Electronic on BreatheHR	Chief Executive, Office Manager, Line Manager Payroll Admin, Connected Voice Business Services Manager Password protected in electronic folders Personnel files are in locked filing cabinet Payroll records are password protected with limited access by finance staff Payroll records kept in locked cabinet with	When staff, start and leave Updated in BreatheHR and kept in password protected folder Chief Executive, Line Manager and Office Manager have access to it Payroll records kept electronically and paper copies – accessed by Payroll Administrator and Business Services Manager	Kept on BreatheHR for duration of employment and up to 6 years afterwards in an archived file	We tell staff that it is used for contact purposes and maintaining sickness records, training, supervisions and appraisals We ask them how they want to receive information from us	Yes	Staff contact details and personal information kept on BreatheHR Staff home addresses are kept on BreatheHR Training records, DBS, medical facts, supervision, appraisals, sickness and leave requests kept on BreatheHR Mobile numbers on BreatheHR with permission of staff member Staff payroll records kept	Start personnel records kept on BreatheHR Password protected only accessed by Chief Executive, Line Manager and Office Manager Staff statistics kept in electronic folder Password protected and only accessed by Chief Executive and Office Manager Personnel correspondence kept in	Duration of employment and for 6 years afterwards HMRC requires us to hold payroll information for 6 years after we have used it. Right to Work data (copy of passport or other right to work documents – eg Biometric visa) kept for duration of employment and for up to 6 years afterwards. Induction data eg key personal data about

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
					access by Payroll Administrator and Business Services Manager					on Sage for seven years	electronic folder when staff member/trustee leaves for duration of employment and up to 6 years afterwards Staff payroll information kept on Sage for 6 years after we have used it Pension data will be kept for the duration of employment and for up to 6 years afterwards	you eg name, address, date of birth, next of kin, bank details, etc kept for the duration of your employment and for up to 6 years afterwards Flexiplanners will be kept for the duration of employment and 6 months afterwards Health and medical data about medical conditions, self-certificates, GP sick notes, consent to gain a report from your GP, consultant or occupational health specialist will be kept for the duration of employment

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
												and up to 6 years afterwards Ethnic monitoring data relating to your racial orgigin, religion, gender, sexual orientation, etc that are classed as protected characteristi c under the Equality Act 2010 will be kept for duration of employment and up to 6 years aafterwards Disciplinary and grievance data will be kept for the duration of employment and up to 6 years afterwards. The warnings will be “live” for the duration specified in them.

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
												Pension data will be kept for the duration of employment and for up to 6 years afterwards 3rd parties who deal with our company benefits, pension, payroll providers may keep this data for longer. Connected Voice will keep it for the duration of your employment and for up to 6 years afterwards Start date, location of workplace, flexible working requests, driving licence details, training records, professional membership, job

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
												performance details, appraisals, supervisions, photographs, use of ICT communication systems will be kept for the duration of your employment and up to 6 years Employees who work on applicable contracts their data will be kept up to the recommended age Future reference data after leaving the organisation including name, address, start and leave dates, job history, last job title and summary of duties, salary details,

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
												training courses attended etc will be kept for the duration of employment and for up to years afterwards
Connected Voice Recruitment Manager, Office Manager Administrator of recruitment	Candidates applying for employment	Contact details, previous jobs, skills, experience, education, volunteering experience, right to work in the UK, outstanding convictions, Ethnic monitoring form	Assessing suitability for employment	Locked filing cabinet Password protected folders	Recruitment Line Manager, Shortlisting Panel, Interview Panel, Administrator	Reviewed at 6 months	Kept for 6 months after an application has been made	Privacy notice given to applicants GDPR statement on application form, job description and ethnic monitoring form	Yes	No	Yes for 6 months after an application has been made then deleted	Yes for 6 months after an application has been made then deleted Successful applicant application form kept for duration of employment and 6 years afterwards
Connected Voice (Chief Executive and Office Manager)	Trustees	Contact details, date of birth, organisation details, bankruptcy declaration for Charity Commission and Companies House Nomination forms	Mailing out information Keeping trustees up to date Board papers Charity Commission and Companies House	Paper files in locked cabinet Contact details on database – password protected Mainly trustee organisation details on database unless	Trustee information password protected Chief Executive, Office Manager, Business Services Manager has access to trustee information	Updated yearly after AGM Paper forms signed and filled in by new trustees Information on new trustees sent to Charity Commission and Companies House	Until resignation from Connected Voice board	Trustees informed at induction how their data will be stored and what it will be used for Trustees given a privacy notice	Yes	Trustees removed from database when they leave Connected Voice board unless they want to receive updates by request	Trustees contact details deleted when they leave Connected Voice Removed from Companies House as a director when resigning	Trustees paper signed forms will be kept until resignation from the board

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
		Trustee agreement Bank signatory information if necessary for the role Declarations of interest Website information	Nomination form used for recruiting new trustees Bank signatories used for authorising payments Adding declarations of interest onto register Skills and experience of trustees for informing the public and stakeholders	trustee has retired or does not work for an organisation		Electronic folder with trustees names and addresses New trustees added to database. Mainly organisation details rather than personal home addresses					from the board Removed from Charity Commission when trustee resigns from the board Website information deleted when trustees resign from the board	
Connected Voice recruitment	Job applicants	Employment application forms Shortlisting assessment forms Interview assessment forms	Recruitment selection	Paper forms in locked drawer Electronic copies of forms in password protected folder	Administrator, Recruitment Panel	Not updated	6 months following recruitment process	Information will be kept confidential	Yes	Not on database	Electronic files kept for 6 months and destroyed	Paper files kept for 6 months and destroyed
Connected Voice (Office Manager)	Connected Voice volunteers	Volunteer form with contact details	Contacting volunteer about Connected Voice work	Locked filing cabinet	Office Manager	Only when new volunteers join Connected Voice	Six years	Information kept confidential to Office Manager , Chief Executive and Volunteer Supervisor	Yes	Information on volunteers kept on BreatheHR	Electronic copies of application forms deleted after six years References kept for six	Volunteer personal information and supervision records kept on BreatheHR for duration

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
											years BreathHR records kept in archived folder for 6 years	of volunteering and kept up to six years afterwards References kept for six years
Connected Voice,(Our Gateshead) (Nominated Gateshead Support Team Lead)	Gateshead Organisations	Organisation contact details (addresses, staff, info in public domain)	To inform residents in Gateshead of organisations and the services they deliver in their area	Our Gateshead	General public	By Nominated Gateshead Support Team Lead and people involved in organisations	As long as subscribed	We tell organisations that their information will be kept on a website database	No – info in the public domain, so no legal right to access data	N/A	N/A	N/A
Connected Voice Advocacy (Manager)	Service users	Personal information (including sensitive personal info)	Case recording and monitoring	Database (Cygnet); paper files; some information on Advocacy drives (L and M) on network	Cygnet has permissions and password access; networks have permissions and network passwords	Cygnet: daily case recording: quarterly as part of monitoring. Paper files: as documents are received.	Thirty years	Section on referral form. Part of initial meeting with client	Yes	Cygnet: records not deleted as used for historical monitoring reports ('relevant' and 'necessary'). Reviewed quarterly	Networks: records not deleted as used for historical monitoring reports ('relevant and necessary'). Reviewed quarterly	Open and Closed clients' records scanned to Cygnet
Connected Voice Advocacy (Manager)	Volunteers	Personal information	Volunteer records and monitoring	Database (Cygnet); paper files	Paid Connected Voice Advocacy staff. As service users	As service users	See Retention columns	Volunteers informed at induction how their data will be stored and kept confidential	Yes	Cygnet: records made inactive when no longer volunteering with us. Not deleted as used for		Open and Closed volunteer records scanned and linked to Breathe HR volunteer record

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
										historical monitoring reports. Reviewed quarterly		
Connected Voice DIY Advocate	App users	Personal information (including sensitive personal info)	To support the user by giving advice and guidance	Stored on a secure encrypted server	User has access to their data through an encrypted password	Data is updated by the user	If the user is active the data is kept indefinitely If the user is inactive for more than 1 year their data is deleted.	Section on app containing the DIY Advocate Data and Privacy Policy	Yes			
Business Services	Clients	Payroll information Accounting information Invoices Records of payments made	Business Services payroll service Managing clients' accounts	Locked cabinet Lever arch files for invoices Sage accountancy and payroll software	Payroll administrator Business Services manager Business Services accountancy assistants	Payroll and accounts mainly updated on Sage software Payroll clients contact details updated on database, Sage software and paper files	Seven years	Information is kept confidential to Business Services	Yes	Payroll clients deleted from Lamplight when they end contract with Business Services Details of clients on Sage software kept for seven years	Business Services clients payroll details and accounts kept on Sage software for seven years	Paper files of payroll clients kept for seven years Paper copies of invoices and accounts kept for seven years
	Customers of Business Services, Support & Development Paid for Services and	Name of organisation Name of individual requesting proposal Organisation	Business Services engaging with customers and managing	Practice Ignition	Michelle Wright Sally Adams Giovanni Spatuzzi Jane Kingston	Updated by Administrators of Practice Ignition	Seven years	Information is kept confidential for the purpose of their account with either Business	Yes	Customer accounts kept for 7 years in line with HMRC	Customer accounts kept for 7 years in line with HMRC	Only electronic files kept on Practice Ignition

Team/ project/ person responsible	Who is the data subject?	What information is collected?	What is the information used for?	How is it stored?	Who has access to it? And is there a password?	How is it updated?	How long is it kept for?	What do you tell the data subject about keeping their data?	Covered by General Data Protection Regulations	Retention: database	Retention: electronic files	Retention: paper files
	Advocacy Service	address Organisation phone number Organisation email address Electronic signature of individual accepting proposal Bank details for direct debit Part credit card details Payroll information Accountancy information Invoices Records of Payments Engagement Letters Quotations	their accounts and preparing quotes Support and Development engaging with customers for managing paid for services and preparing quotes Advocacy DIY Advocate app for engaging with customers to purchase DIY advocate and preparing quotes	Practice Ignition Practice Ignition	Melissa Girling Tracey Gray Permission levels Standard and Administrator Administrators have access to everything in the Practice Ignition Account Michelle Wright Administrator Sally Adams Administrator Standard Users have limited access Giovanni Spatuzzi Jane Kingston Melissa Girling Tracey Gray			Services, Support and Development or Advocacy Service depending on customer's purchase				