CONNECTED VOICE
EMPLOYEE DATA PROTECTION AND PRIVACY POLICY

Introduction

This policy sets out information in relation to the processing of employee data and how employee privacy of data is protected. This policy does not confer any contractual rights.

Connected Voice is a "data controller" and needs to collect and hold data about you to enable us to administer day to day tasks related to your ongoing employment (e.g. we need to know your bank detail in order that we can pay you).

Connected Voice is permitted to hold and process data about you because you are an employee/worker and there is a contract between us (the main legal basis for processing your information).

Connected Voice' obligations in relation to the processing of personal data

Connected Voice is required to ensure that it complies with the following obligations when processing any of your personal data:

- that your data is used lawfully, fairly and in a transparent way
- that your data is collected only for valid purposes which have been clearly explained to you
- that the data collected is relevant to the purposes Connected Voice has told you about and limited only to those purposes
- that the data is accurate and up to date
- that your data is kept in a format which allows for you to be identified for only as long as necessary
- that your data is kept securely

Connected Voice will only use your personal data for the stated purposes, unless there is a need to use it for another reason and that reason is compatible with the original purpose. If the Connected Voice considers that it is necessary to use your personal data for a different and unrelated purpose, this will be notified to you in writing with an explanation of the legal basis for doing so. There may be exceptional circumstances where Connected Voice has to process your personal data without your knowledge or consent where this is required by law.

Connected Voice will only ask you to provide data which is necessary for the performance of the contractual employment relationship or any associated legal obligations. If you do not provide this data, Connected Voice may not be able to meet its contractual or legal obligations to you.

For Connected Voice to meet the obligations of managing your contract or to meet legal obligations connected with your employment relationship, it is necessary to share your personal information with certain third parties (e.g. payroll provider, pension provider, legal or professional advisers). Connected Voice may also share your personal data with other third parties (e.g. through Transfer of Undertakings Protection of Employment). Connected Voice does not transfer personal data outside the EEA.

Individual rights and obligations

Current data protection legislation provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

In order that we can ensure that the personal data we hold in relation to you is accurate, it is important that you keep us informed of any changes to your data.

How personal data is collected

Connected Voice collects your personal data by a variety of means. At the recruitment stage Connected Voice will already have collected data through the application process and references from current or former employers.

Where any additional personal data is required, Connected Voice will ask you for this in writing, setting out the purpose for which is it required.

The type of data Connected Voice may process

The data processed includes, but is not limited to:

Type of data	Why we wish to hold it	How long it will be kept for
Recruitment data Previous employers, types of job held previously, skills and qualifications, CV	This will allow us to make a decision on your suitability for employment/ engagement.	Data obtained during recruitment will be kept for six months after an application has been declined. If appointed data will be kept for the duration of your employment and for nine months afterwards.
Contract of employment	This is a record of terms and conditions so that both employer and employee have a signed agreement.	The contract of employment will be kept in the employee's personnel file for duration of their employment and seven years afterwards.
Right to work Copy of passport (or other right to work documents –e.g. Biometric visa)		This data will be kept for the duration of your employment and for two years afterwards.
Induction data Key personal data about you: e.g. name address, date of birth, next of kin, bank details, etc.	This will allow us to send you correspondence, contact next of kin in an emergency, pay wages into your bank, enrol you into benefits schemes etc.	This data will be kept electronically on Breathe HR for the duration of your employment and for nine months afterwards.
Payroll data	To allow us to pay you	The HMRC requires us to hold this

Salary and salary history, benefits, tax, NI and NI number, tax status, pension contributions, other deductions, student loans, timesheets, CCJ's etc.	accurately, via our third-party payment provider, and to fulfil out tax and reporting obligations with the HMRC.	information for six years after we have used it.
Time and attendance data Flexplanner system	To allow us to ensure you are working the correct hours and that obligations under the Working Time Regulations are met.	This data will be kept for the duration of your employment and for nine months afterwards.
Health and medical data Data about your health, medical conditions, self-certificates, GP sick notes Your consent may also be sought to gain a report from your GP, consultant or occupational health specialist.	We may need to understand details about health / medical conditions in relation to your work and ability to undertake your role, or alternative roles. We would only seek this information from you with your specific consent.	This data will be kept for the duration of your employment and for nine months afterwards. If it relates to an accident at work, we would keep the data for four years after your employment has ended
Ethnic monitoring data Data relating to your racial origin, religion, gender, sexual orientation, etc that are classed as protected characteristics under the Equality Act 2010.	We use this data to understand the diversity of our workforce and it allows us to rebalance our workforce if we believe we do not have the correct diversity.	This data will be kept for the duration of your employment and for nine months afterwards.
Disciplinary and grievance records	These will be kept on file as a reference for comparison purposes to ensure any requirements to improve your conduct or capability can be referenced.	This data will be kept for the duration of your employment and for nine months afterwards. The warnings will be 'live' for the duration specified in them.
Other data Start date, location of workplace, flexible working requests, driving licence details, training records, professional memberships, job performance details, appraisals, supervision notes, CCTV, photographs, use of IT/ communication systems etc.	We might need to calculate entitlements to benefits or rights arising from length of service, understand details about work performance, training needs, policy compliance etc., or making decisions about promotion or continued employment.	This data will be kept for the duration of your employment and for nine months afterwards.
Third parties who deal	If you enrol in a company	This data will be kept for the

with our company benefits Pension, payroll providers etc.	benefit, we will need to share certain data with a third party to allow them to process your benefits.	duration of your employment and for nine months afterwards. The third party may keep this data longer (e.g. pension provider holding your information).
Future reference data (after you have left Connected Voice) Key data items: name, address, start and leave dates job history, last job title and summary of duties, salary details, training courses attended etc.	We would keep a small amount of basic data about you (after you had left) that would allow us to give a prospective employer a reference.	This data will be kept for the duration of your employment/engagement and for up to five years afterwards. References requested and provided after employees have left the organisation will be kept for twelve months and then destroyed.
DBS checks Certificates and risk assessments	DBS checks will be carried out if a post is eligible. Careful consideration will be given to whether the post is eligible before a DBS check is requested. Connected Voice contracts with commissioners require some posts to be DBS checked because of regulated activity. A risk assessment will be carried out if a DBS certificate shows a criminal conviction in line with the Connected Voice Disclosure and Barring Policy and Procedure Connected Voice will hold this information to be compliant with commissioners' contracts.	A negative DBS certificate (one that shows no criminal convictions) will be recorded on the Connected Voice DBS log. This information will be kept for the duration of employment and for seven years afterwards A positive DBS certificate (one that shows a criminal conviction(s) will require a risk assessment to be carried out. If Connected Voice decides to go ahead with the employment/retain the employee then the risk assessment and the DBS certificate will be kept for the duration of the employment and seven years afterward.
Contracts and supporting guidelines	We may be required to keep employee data longer to comply with contractual obligations.	For those employees who have worked on applicable contracts their data will be kept up to the recommended age.

When Connected Voice will use your personal data

Generally, Connected Voice will use your personal data for one of the following lawful reasons:

- to perform the contract we have entered into with you
- to comply with a legal obligation

- where it is necessary for legitimate interests (or those of a third party)

There are other rare occasions where your personal data or special category data will be used:

- where we need to protect your interests (or someone else's interests)
- where it is needed in the public interest, or where it has already been made public
- where Connected Voice has to process this data for legal claims

Special category data

Any personal data which identifies ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation is classed as special category data. Connected Voice will only use this data:

- to comply with employment and other laws when processing and managing situations connected with absences arising in relation to your sickness or family/ dependant related leave etc.
- to ensure health and safety compliance
- to assess your capability to perform your role, monitor and manage your sickness absence, provide appropriate workplace adjustments etc.
- Where it is needed in the public interest, for example for equal opportunity monitoring and reporting

In limited circumstances, Connected Voice may request your written consent to allow us to process special category data (e.g. for the purpose of gaining a medical report).

Connected Voice does envisage that it will hold data about criminal convictions. Connected Voice will only collect data about criminal convictions if it is appropriate to role and duties you will perform.

Automated decision making

Connected Voice will only collect data about criminal convictions if it is appropriate to the role and duties you will perform.

Subject Access Requests

You are entitled to make a subject access request (SAR). Any request should be made in writing to the Chief Executive. If you make an SAR, Connected Voice we may request specific information to confirm your identity to ensure that the data is released to the correct person.

The information will be provided in a commonly-used electronic form, unless otherwise requested by the individual.

Connected Voice will respond to an SAR within 30 calendar days, with a possibility to extend this period for particularly complex requests. Connected Voice may withhold personal data if disclosing it would 'adversely affect the rights and freedoms of others'.

Connected Voice will only charge you a fee for an SAR if your request is 'manifestly unfounded or excessive', or if further copies of data are requested.

Data breaches

Where any personal data is lost, destroyed, corrupted or disclosed etc. this will amount to a data breach.

In the event of a data breach, staff must immediately inform their line manager.

In the rare event that a data breach occurs Connected Voice will investigate the cause of any breach, determine any remedial action that can be taken and consider how the effect of the breach can be mitigated.

Initial priorities for Connected Voice are to:

- contain the breach
- assess the potential adverse consequences for the individual(s), based on how substantial these are

Where personal data has been sent to someone who is not authorised to have access to it, Connected Voice will:

- inform the unauthorised recipient not to distribute it in any way or discuss it with anyone else
- inform the unauthorised recipient to destroy or delete the data
- require the unauthorised recipient to confirm in writing that they have destroyed/ deleted the data
- advise the unauthorised recipient of the implications if they disclose the data
- where relevant, inform the data subject(s) so that they can take any necessary action

When a personal data breach has occurred, Connected Voice needs to establish the likelihood and severity of the risk to individual(s) rights. If there is a risk, then Connected Voice will notify the ICO. In the event that a risk is unlikely the there is no requirement for Connected Voice to report it to the ICO.

Notifiable breaches must be reported to the ICO no later than 72 hours after Connected Voice became aware of it.

15 October 2025