Privacy Policy

Reviewed: August 2025
Next review due: August 2028, *unless there is a change to the data we collect or how we use it*

Purpose

This Privacy Policy covers all aspects of how Better Connect operates outside of any specific programme. This means this policy relates to:

1. Employees of Better Connect
2. Non-Executive Directors of Better Connect
3. Individuals contacting Better Connect about working with us
4. Individuals applying for jobs with us

Each programme will have a separate Privacy Notice for participants and delivery partners, which will include information about the data collected and retention periods that apply to that programme. The same principles will apply.

At Better Connect we understand the importance of meeting our contractual, statutory and administrative obligations. We are committed to ensuring that the personal data we hold is handled in line with the Data Protection Act 2018, which incorporates the UK General Data Protection Regulation (GDPR). This Privacy Policy outlines your privacy rights, and how we gather, use and share personal data about you during and after your working relationship with us.

This policy is updated with any relevant changes to the legislation as required from time to time. If significant changes are made to what data we collect or how we use it we will let you know. There may also be times when additional data is collected and processed, and we will provide other specific privacy notices as required so that you know how and why we are collecting that data.

Data controller and data processor

We, Better Connect Limited, are the data controller of the personal information we gather and use for our own purposes. We are the data processor of the personal information we gather and use at the direction of funders or organisations who have a legal or contractual obligation to that data.

For most data outlined in this policy we are the Data Controller.

We are a Data Processor for data that we must legally pass to HMRC (employees) and Companies House (Directors). Data collected at the direction of funders is outlined in the individual programme Privacy Notices.

Your data protection rights

Under data protection law, you have rights including:

- Your right of access
  You have the right to ask us for copies of your personal information.
- Your right to rectification
  You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- Your right to erasure
  You have the right to ask us to erase your personal information in certain circumstances.
- Your right to restriction of processing
  You have the right to ask us to restrict the processing of your personal information in certain circumstances.
- Your right to object to processing
  You have the right to object to the processing of your personal information in certain circumstances.
- Your right to data portability
  You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

If you make a request, we have one month to respond to you, and will make every effort to respond much more quickly. You should contact the Head of Operations if you wish to make a request.

Use of Artificial Intelligence (AI)

In line with our Artificial Intelligence Policy, only anonymised data is permitted to be used with AI. We will never use AI to make any automated decision that impacts an individual. As such no information that could identify an individual is permitted to be used with AI by any member of the Better Connect team.

1. **Employees of Better Connect**

For employees of Better Connect, this notice does not form part of your employment contract and it may be amended at any time.

The information collected

We currently collect and process the following information:

- Personal contact details such as name, job title, home addresses, telephone numbers, and personal email addresses
- Date of birth
- Equality monitoring data not considered special category data (e.g. gender)
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Employment start date

- Location of employment or workplace
- Identification information (for example a copy of driving licence, passport and utility bills).
- Recruitment information (including copies of right to work documentation, references and other information provided as part of the application process)
- Employment records (including job titles, work history, working hours, flexible working requests, training records and professional memberships)
- Compensation history
- Performance information
- Disciplinary and grievance information
- Data relating to the administration of events and activities (for example Team Day lunch orders or survey responses)

Some kinds of personal data are given special protection by law, and are called 'special category' data. We will sometimes collect, store and use the following types of **special category data**:

- Information about your race or ethnicity, religious beliefs, and sexual orientation
- Information about your health, including any medical condition, health and sickness records
- Information about your criminal convictions and offences (if disclosed to us, we do not currently undertake Disclosure and Barring Service checks)

How we collect and use the information

Most of the personal information we collect is provided to us directly by you for one of the following reasons:

- It enables us to meet our statutory obligations when you begin working for us as an employee
- It enables us to meet our legal obligations as a company
- It enables us to provide the support you need
- It enables you to fully participate in events or activities that we offer to the team

We may share this information with external organisations or individuals who need it to provide a service to us. Only the minimum personal information they need would be provided. Those with whom we would share information are:

- Suppliers who need to identify individual employees
- Training providers
- IT suppliers setting up user accounts
- Funders for processing applications or claims
- Organisations with which we are required by law to share information (e.g. HMRC)
- Organisations who support us in our employment relationship with you (e.g. payroll, or HR advice)

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are:

- Your consent
  You are able to remove your consent at any time in certain circumstances, and you can do this by contacting the Head of Operations
- Where we have a contractual obligation
- Where we have a legal obligation

- Where we have a legitimate interest

We do not need your consent to use your personal data where there is another legal basis for using it. Where we need your consent we will give you full details of the information we are requesting and why we need it so you can decide whether to give your consent. In these circumstances you are under no obligation to give your consent and may withdraw it at any time.

Unless the **special category data** needs to be identifiable to you, such as if we need to make an adjustment for a declared health condition, we will collect and store this data anonymously. Equality and inclusion monitoring data will usually be treated in this way. When we collect special category data we will make it clear if it will be identifiable or anonymous.

We only process your special category data with your consent or where we have an obligation to do so as your employer.

A Data Protection Impact Assessment (DPIA) has been considered. The scope of the data we collect and use from employees is not considered to pose a risk high enough to warrant a DPIA at this time. Data security measures continue to be taken, and whether a DPIA is needed will be kept under review. This decision was informed by the ICO's guidance on DPIAs: Data protection impact assessments | ICO

How we store your personal information

Your information is securely stored:

- in a locked cabinet in the office (only where physical copies exist), only the Head of Operations has the key
- on our Sharepoint (Microsoft 365) site with access restricted only to people who need access to specific folders
- on our digital HR platform (for staff only) – Bright HR – where access is restricted to you or your Line Manager, and designated administrators.

You should refer to our Confidentiality and Data Protection Policy for details on how long we retain each type of data.

Some funding agreements require us to keep relevant employee records for longer, and where this affects any of your information, you will receive a separate notice to let you know.

Withholding personal data

If you choose to withhold any personal data that we ask for, we may not be able to fully meet the terms of the employment contract we have with you, or we may be prevented from meeting our legal or statutory obligations. In certain circumstances this may impact upon your continued employment with us. We will always let you know why we need the data we are requesting.

Employee Concerns or Complaints

We encourage all concerns to be raised with the Head of Operations or CEO as early as possible so they can be resolved quickly. If you have any concerns about our use of your personal information, you can make a complaint to the CEO.

2. Non-Executive Directors of Better Connect

The information collected

We currently collect and process the following information:

- Personal contact details such as name, job title, home addresses, telephone numbers, and email addresses
- Date of birth
- Equality monitoring data not considered special category data (e.g. gender)
- Nationality
- Occupation
- Identification information (for example a copy of driving licence, passport and utility bills).
- Recruitment information (including references and other information provided as part of the application process)
- Other directorships
- Data relating to the administration of events and activities (for example lunch orders or survey responses)

Some kinds of personal data are given special protection by law, and are called 'special category' data. We will sometimes collect, store and use the following types of **special category data**:

- Information about your race or ethnicity, religious beliefs, and sexual orientation
- Information about your health, including any medical condition, health and sickness records
- Information about your criminal convictions and offences (if disclosed to us, we do not currently undertake Disclosure and Barring Service checks)

How we collect and use the information

Most of the personal information we collect is provided to us directly by you for one of the following reasons:

- It enables us to meet our statutory obligations when you begin working with us as a Non-Executive Director
- It enables us to meet our legal obligations as a company
- It enables us to provide the support you need
- It enables you to fully participate in events or activities that we offer to Directors

We may share this information with external organisations or individuals who need it to provide a service to us. Only the minimum personal information they need would be provided. Those with whom we would share information are:

- Organisations with which we are required by law to share information (e.g. Companies House)
- IT suppliers setting up user accounts
- Training providers
- Suppliers who need to identify individual Non-Executive Directors

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are:

- Your consent
  You are able to remove your consent at any time in certain circumstances, and you can do this by contacting the Head of Operations

- Where we have a legal obligation
- Where we have a legitimate interest

We do not need your consent to use your personal data where there is another legal basis for using it. Where we need your consent we will give you full details of the information we are requesting and why we need it so you can decide whether to give your consent. In these circumstances you are under no obligation to give your consent and may withdraw it at any time.

Unless the **special category data** needs to be identifiable to you, such as if we need to make an adjustment for a declared health condition, we will collect and store this data anonymously. Equality and inclusion monitoring data will usually be treated in this way. When we collect special category data we will make it clear if it will be identifiable or anonymous.

We only process your special category data with your consent or where we have an obligation to do so as your employer.

A Data Protection Impact Assessment (DPIA) has been considered. The scope of the data we collect and use from Directors is not considered to pose a risk high enough to warrant a DPIA at this time. Data security measures continue to be taken, and whether a DPIA is needed will be kept under review. This decision was informed by the ICO's guidance on DPIAs: Data protection impact assessments | ICO

How we store your personal information

Your information is securely stored:

- on our Sharepoint (Microsoft 365) site with access restricted only to people who need access to specific folders

Directors are potentially liable for any penalty arising from an act or infringement at the time they were a Director, even if they subsequently resigned. For this reason we will retain Non-Executive Director contact details for no more than 7 years after resignation from the Board. All other information, such as identification documents you provided to us when you joined the Board, will be deleted upon resignation.

All Directors must be registered on Companies House. Companies House keep this information publicly available for the lifetime of the company, and for 20 years after the company is dissolved.

Withholding personal data

If you choose to withhold any personal data that we ask for, we may be prevented from meeting our legal or statutory obligations. In certain circumstances this may impact upon your continued role as Non-Executive Director with us. We will always let you know why we need the data we are requesting.

Director Concerns or Complaints

We encourage all concerns to be raised with the Head of Operations or CEO as early as possible so they can be resolved quickly. If you have any concerns about our use of your personal information, you can make a complaint to the CEO.

3. Individuals contacting Better Connect about working with us

This section relates to the data we collect, process and store about individuals who contact us about working with Better Connect as a delivery partner or supplier, for example. The amount of personal information we collect from you should be minimal, as we will only need professional information linked to your work. However, this can still identify you as a person and is therefore considered personal information.

The data that we currently collect and process in this sense is:

- Individual contact details, including email address, phone number and job title
- Contact details for your organisation
- Relevant information about your skill or experience that relates to the work you would like to do with us

How we collect and use the information

Most of the personal information we collect is provided to us directly by you for one of the following reasons:

- It enables us to contact you about opportunities to work with us
- It enables us to determine if we will work with you

We may share this information with external organisations or individuals who need it to provide a service to us. Only the minimum personal information they need would be provided.

We may also recommend another organisation within our trusted network contact you where your professional interests align with their needs. In these instances, we will only provide your name, organisation and any workplace contact detail we hold for you.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are:

- Your consent
  You are able to remove your consent at any time in certain circumstances, and you can do this by contacting the Head of Operations (suppliers) or Head of Business Development (delivery partners)
- Where we have a legitimate interest

We do not need your consent to use your personal data where there is another legal basis for using it. Where we need your consent we will give you full details of the information we are requesting and why we need it so you can decide whether to give your consent. In these circumstances you are under no obligation to give your consent and may withdraw it at any time.

How we store your personal information

Your information is securely stored:

- on our Sharepoint (Microsoft 365) site with access restricted only to people who need access to specific folders
- in our JotForm account with access restricted to members of the team who need access to the information collected by that specific form (applications to become a delivery partner)

Withholding personal data

If you choose to withhold any personal data that we ask for, we may be unable to work with you. We will always let you know why we need the data we are requesting.

Concerns or Complaints

We encourage all concerns to be raised with the Head of Operations or CEO as early as possible so they can be resolved quickly. If you have any concerns about our use of your personal information, you can make a complaint to the CEO.

4. Individuals applying for jobs with us

The information collected

We currently collect and process the following information:

- Personal contact details such as name, home address, telephone numbers, and personal email addresses
- Information about your career history, education, skills and experience
- Equality monitoring data not considered special category data (e.g. gender)
- Identification information (for example a copy of driving licence, passport and utility bills).
- Recruitment information (including copies of right to work documentation, references and other information provided as part of the application process)

Some kinds of personal data are given special protection by law, and are called 'special category' data. We will sometimes collect, store and use the following types of **special category data**:

- Information about your race or ethnicity, religious beliefs, and sexual orientation
- Information about your health
- Information about your criminal convictions and offences (if disclosed to us, we do not currently undertake Disclosure and Barring Service checks)

How we collect and use the information

Most of the personal information we collect is provided to us directly by you for one of the following reasons:

- It enables us to contact you about the recruitment process and other job opportunities
- It enables us to assess your application against the requirements of the job description
- It enables us to meet our legal obligations as a company
- It enables us to provide the support you need to do your best in the selection activities

We may share some of this information with the references you provide to us in order that they may accurately identify you and provide an appropriate reference to us. We will only contact references if you are offered the job and once you tell us we may contact them.

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are:

- Your consent
  You are able to remove your consent at any time in certain circumstances, and you can do this by contacting the Head of Operations
- Where we have a contractual obligation
- Where we have a legal obligation
- Where we have a legitimate interest

We do not need your consent to use your personal data where there is another legal basis for using it. Where we need your consent we will give you full details of the information we are requesting and why we need it so you can decide whether to give your consent. In these circumstances you are under no obligation to give your consent and may withdraw it at any time.

Unless the **special category data** needs to be identifiable to you, such as if we need to make an adjustment for a declared health condition, we will collect and store this data anonymously. Equality and inclusion monitoring data will usually be treated in this way. When we collect special category data we will make it clear if it will be identifiable or anonymous. We only process your special category data with your consent.

A Data Protection Impact Assessment (DPIA) has been considered. The scope of the data we collect and use from job applicants is not considered to pose a risk high enough to warrant a DPIA at this time. Data security measures continue to be taken, and whether a DPIA is needed will be kept under review. This decision was informed by the ICO's guidance on DPIAs: Data protection impact assessments | ICO

How we store your personal information

Your information is securely stored:

- in a locked cabinet in the office (only where physical copies exist), only the Head of Operations has the key
- on our Sharepoint (Microsoft 365) site with access restricted only to people who need access to specific folders

In line with our Confidentiality and Data Protection Policy we only retain information about job applicants for set periods of time:

- Candidates not shortlisted have their information deleted two weeks after we notify them
- Candidates unsuccessful at interview have their information deleted six months after we appoint the role
- Successful candidates' information is moved to their employee file and is retained in line with the retention period for employees.

Withholding personal data

If you choose to withhold any personal data that we ask for, we may not be able to fully assess your application, or we may be prevented from meeting our legal or statutory obligations. In certain circumstances this may impact upon the success of your job application. We will always let you know why we need the data we are requesting.

Applicant Concerns or Complaints

We encourage all concerns to be raised with the Head of Operations or CEO as early as possible so they can be resolved quickly. If you have any concerns about our use of your personal information, you can make a complaint to the CEO.

Contact Details

We ask that any requests or concerns about your data are directed to the Head of Operations or the CEO. They can be reached through the following contact details:

Head of Operations: Deborah Chaddock, dchaddock@betterconnect.org.uk

CEO: Natasha Babar-Evans, nbabarevans@betterconnect.org.uk

Information Commissioners Office

We encourage anyone with concerns or complaints about how we have handled their data to contact us directly in the first instance. If you are unhappy with how we respond to you, you can also complain to the ICO.

The ICO's address:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk