Data Protection and Confidentiality Policy

Supportive Bridge Ltd | Community Support and Healthcare Staffing | Bradford, England

POLICY AT A GLANCE

- **Need to know only.** Share personal information with people who need it to do their job, and share the minimum needed.
- **Never discuss people we support** where others can hear, with your own family and friends, or on social media. No photographs on personal phones.
- **Safeguarding overrides confidentiality.** If someone is at risk of harm, report it. You never need consent to raise a safeguarding concern.
- **Lost or misdirected information must be reported to the Registered Manager immediately,** at any hour. Serious breaches must reach the ICO within 72 hours.
- **People can see what we hold about them.** Any request for copies goes to the Registered Manager the same day, and we must reply within one month.
- **Keep it secure:** locked cabinets, passworded devices, no personal email or WhatsApp for work information, nothing left in a car.
- **The company must be registered with the ICO** and pay the annual data protection fee.

SERVICE DETAILS (fill in before issuing)

Registered Manager	
Nominated Individual	
Data protection lead	
ICO registration number	
Office phone	
Date issued	
Next review date	

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.

1. PURPOSE

1.1 This policy explains how Supportive Bridge Ltd ("Supportive Bridge", "we", "us") protects the personal information we hold about the people we support, our workers and everyone else we deal with, and how we meet the UK General Data Protection Regulation and the Data Protection Act 2018.

1.2 It also sets out the common law duty of confidentiality, which applies to everything our workers see and hear in people's homes, whether or not it is written down.

1.3 It supports Regulation 17 (Good governance) of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.

2. SCOPE

2.1 Supportive Bridge Ltd operates two arms, and this policy applies to both: our **healthcare staffing service**, supplying care and support workers to care homes, hospitals and other providers; and our **community support service**, where our own support workers visit adults and older people in their own homes, including council housing, on morning and evening shifts, to support them with daily living.

2.2 Supportive Bridge does **not** provide personal care. Personal care is a regulated activity under the Health and Social Care Act 2008 and we will provide it only if and when we are registered with the Care Quality Commission. Our support workers provide non-personal support such as companionship, meal preparation, shopping, domestic help, prompting, and support to get out and about. This policy is written to meet both local authority provider assurance requirements and the standards we will be assessed against at CQC registration.

2.3 It applies to everyone who works for us and to all personal information we hold, in any form: paper, electronic, photographs, recordings, emails, text messages and conversations.

2.4 Supportive Bridge is the **data controller** for the information it holds. Where we supply workers to a client organisation, that organisation is normally the controller for information about the people it supports, and our workers must follow its policies; we remain controller for our own worker records.

2.5 Deliberately misusing personal information may be a criminal offence as well as gross misconduct.

3. THE DATA PROTECTION PRINCIPLES

3.1 Personal information must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes, and not used in a way incompatible with those;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept no longer than necessary;
- kept securely, protected against unauthorised access, loss or damage.

3.2 We must also be able to **demonstrate** that we meet these principles. That is why we keep records of what we hold, why, and who we share it with.

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.

4. KEY TERMS

Term	What it means
Personal data	Any information that identifies a living person, directly or indirectly: name, address, date of birth, NHS number, photographs, or notes about them.
Special category data	More sensitive information needing extra protection: health, race or ethnic origin, religion, sexual orientation, sex life, political opinions, trade union membership, genetics and biometrics. Almost everything in a support record is special category data.
Criminal offence data	Information about convictions, cautions and alleged offences, including DBS results. It has its own additional conditions.
Controller	The organisation that decides why and how personal data is used. Supportive Bridge is a controller.
Processor	An organisation that processes data on our instructions, such as a care records software supplier or payroll provider.
Data subject	The person the information is about.
Personal data breach	Any loss of, unauthorised access to, alteration or wrongful disclosure of personal data, whether deliberate or accidental.

5. OUR LAWFUL BASES

5.1 We must have a lawful basis for everything we do with personal data, and an extra condition for special category and criminal offence data.

What we do	Lawful basis	Extra condition
Providing support to a person	Contract, and legal obligation	Provision of health or social care (Article 9(2)(h)), with the Data Protection Act 2018 Schedule 1 condition
Safeguarding an adult or child at risk	Legal obligation, or vital interests where life is at risk	Safeguarding of children and individuals at risk (Schedule 1, Part 2)
Employing and vetting staff	Contract, and legal obligation	Employment, social security and social protection; and for DBS, prevention or detection of unlawful acts
Sending marketing or newsletters	Consent	Not applicable
CCTV or recordings, where ever used	Legitimate interests, assessed	As applicable

5.2 Note that we do **not** rely on consent to deliver support or to keep records. Consent must be freely given and capable of being withdrawn, and someone receiving support is not in a position to withdraw consent to being recorded about. Consent is still asked for, and recorded, where we share information beyond what the law requires, for example with a family member.

6. CONFIDENTIALITY IN PRACTICE

6.1 Every worker owes a duty of confidence to the people we support. In practice this means:

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.

- do not discuss one person with another person we support, with neighbours, or with visitors;
- do not discuss people we support with your own family or friends, even without names; local details identify people easily;
- do not talk about work on the bus, in a shop, in a waiting room, or on a hands-free call in the car;
- never post about work, the people we support, their homes or their families on social media, and never accept a person we support or their family as a friend or follower on a personal account;
- never take photographs or video of a person, their home, their records or a screen on a personal phone. Where a photograph is genuinely needed, it is taken on a company device, with consent or a recorded best interests decision, at the Registered Manager's direction;
- do not look at records for anyone you are not supporting;
- keep paperwork out of sight in the home, in the car and in the office.

6.2 We follow the Caldicott principles: have a clear purpose for using confidential information, use the minimum necessary, access it on a strict need-to-know basis, be aware of your responsibilities, comply with the law, and remember that the duty to share information can be as important as the duty to protect it.

7. WHEN WE SHARE INFORMATION

7.1 We share personal information:

- with other professionals involved in a person's care, such as their GP, district nurse, pharmacist or social worker, where it is needed for their care;
- in an emergency, for example telling paramedics about a person's conditions and medicines;
- to protect someone from harm, under our Safeguarding Adults Policy. **A safeguarding concern is always reported, with or without consent**;
- with the local authority or NHS body funding the support, to the extent set out in the contract;
- with a client organisation, about a worker we supply, limited to what the Conduct Regulations require;
- with regulators such as CQC, the ICO, the HSE or the police, where we are required or permitted to;
- with a person's family or representative, only to the extent the person has agreed, or where they lack capacity and it is in their best interests.

7.2 Every disclosure is recorded: what was shared, with whom, when, why, and the lawful basis. Where information is sent by email, it is sent to a secure or verified address, encrypted or password protected where it contains sensitive detail, and the address is double-checked before sending.

7.3 We do not sell personal data or use it for marketing without consent.

8. KEEPING INFORMATION SECURE

- paper records are kept in locked cabinets in a secure office; the office is locked when unattended;
- electronic records are held on password-protected, encrypted systems with individual logins, multi-factor authentication where available, and regular backups;
- each worker has their own username and password, which must never be shared or written down;
- devices are locked with a PIN, passcode or biometrics, and locked whenever put down;
- work information must never be sent through personal email, WhatsApp or other personal messaging apps, or stored on personal devices or personal cloud accounts;

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.

- records are never left in a car, taken home, or left visible in a person's home;
- screens are positioned so they cannot be overlooked;
- access is limited to those who need it, and is removed the day someone leaves;
- confidential waste is cross-cut shredded or destroyed by a confidential waste service.

8.1 Where we use a supplier who handles personal data for us, such as care records software, payroll or an accountant, we check their security, put a written contract in place with the terms required by UK GDPR Article 28, and satisfy ourselves that data stays within the UK or is transferred only under approved safeguards.

9. PEOPLE'S RIGHTS

9.1 People have the right to be informed, to see their information, to have it corrected, and in some circumstances to have it erased, restricted or ported, and to object to certain uses. Our Privacy Notice explains this and is given to every person we support and every worker.

Subject access requests

9.2 Anyone can ask for a copy of the information we hold about them. A request can be made in any way, including verbally, to any member of staff.

- any request is passed to the Registered Manager the **same day**;
- we respond within **one calendar month**, free of charge. This can be extended by two months for complex requests, and we must tell the person within the first month if so;
- we confirm the person's identity before releasing anything;
- we check what must be removed first, in particular information about other people who have not consented, and we record what was withheld and why;
- where someone asks on another's behalf, we check their authority and, where the person has capacity, their consent.

9.3 Requests for correction are dealt with within one month. We do not delete an entry that has been made in a support record, because that would falsify the record; instead we add a note recording the correction and who made it.

10. RETENTION AND DISPOSAL

10.1 We keep information only as long as we need it:

Record	How long we keep it
Support records for an adult	8 years after support ends, or after death
Safeguarding records	At least 8 years, or longer if the local authority or an investigation requires
Staff personnel files	6 years after employment ends
Recruitment records for unsuccessful applicants	6 months
DBS certificate copies	Not kept beyond 6 months
Accident book and RIDDOR records	At least 3 years
Complaints records	At least 6 years

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.

Record	How long we keep it
Payroll and tax records	6 years

10.2 At the end of the retention period, paper is cross-cut shredded and electronic records are securely deleted. The Registered Manager records what was destroyed, when and how.

11. DATA BREACHES

11.1 A breach is any loss of, unauthorised access to, or wrongful disclosure of personal information. Common examples are a lost folder or phone, an email sent to the wrong address, records left in a car, a conversation overheard, or a password shared.

IF YOU THINK THERE HAS BEEN A BREACH

1. Tell the Registered Manager **immediately**, at any hour. Do not wait until your next shift.
2. Do what you can to limit the harm: recall the email, retrieve the paperwork, change the password.
3. Write down exactly what happened, when you noticed, and what information was involved.
4. Do not try to cover it up. Reporting quickly and honestly is what matters, and no one will be disciplined for an honest mistake reported promptly.

11.2 The Registered Manager records the breach on the breach log, assesses the risk to the people affected, takes action to contain it, and decides whether it must be reported.

- A breach likely to result in a risk to people's rights and freedoms must be reported to the Information Commissioner's Office **within 72 hours** of us becoming aware of it;
- where there is a high risk to the individual, we tell them too, without undue delay, in plain language;
- we record every breach, including those we decide not to report, and the reasons;
- a serious breach may also require a CQC notification, a safeguarding referral, and action under our Duty of Candour Policy.

12. GOVERNANCE

12.1 The Registered Manager is responsible for data protection day to day, supported by the data protection lead named on page 1. We are not required to appoint a statutory Data Protection Officer at our current size, and we will review that if our activities change.

12.2 The company is registered with the Information Commissioner's Office as a data controller and pays the annual data protection fee. The registration number is recorded on page 1 and shown on our privacy notice.

12.3 We keep a record of our processing activities, describing what data we hold, why, who we share it with, how long we keep it and how it is protected, and we review it at least annually. Where a new system or way of working is likely to be high risk, we complete a data protection impact assessment before starting.

13. TRAINING

13.1 All workers complete data protection and confidentiality training at induction, before handling any personal information, and refresh it every year. Training covers confidentiality in people's homes, social media, secure handling of records, subject access requests and breach reporting.

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.

13.2 Confidentiality is written into every contract of employment, and a breach of it may be gross misconduct.

14. MONITORING AND REVIEW

14.1 The Registered Manager audits record security and confidentiality practice during spot checks and monthly record audits, and reviews the breach log monthly. The Nominated Individual reviews a summary at least quarterly.

14.2 This policy is reviewed every year, or sooner if the law or ICO guidance changes, or after any significant breach.

15. LEGISLATION AND GUIDANCE

- UK General Data Protection Regulation
- Data Protection Act 2018, including Schedule 1 conditions for special category and criminal offence data
- Common law duty of confidentiality and the Caldicott principles
- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, Regulations 17 and 20
- Care Act 2014 and the Care and Support Statutory Guidance on information sharing
- Mental Capacity Act 2005
- Human Rights Act 1998, Article 8
- Privacy and Electronic Communications Regulations 2003
- Computer Misuse Act 1990
- NHS Records Management Code of Practice (retention)
- Information Commissioner's Office guidance on subject access, breach reporting and the data protection fee

16. RELATED POLICIES AND FORMS

Related policies: Support Records and Record Keeping; Safeguarding Adults; Consent and Mental Capacity; Complaints, Concerns and Compliments; Duty of Candour; Social Media and Mobile Phones; Staff Code of Conduct; Safer Recruitment, Selection and DBS; Business Continuity; Whistleblowing.

Forms: Privacy Notice (people we support, and staff); Record of Processing Activities; Consent to Share Information; Subject Access Request Log; Data Breach Record (Appendix A); Data Protection Impact Assessment template.

17. DOCUMENT CONTROL

Version	Date	Approved by	Role	Reason
1.0			Nominated Individual	New policy for local authority assurance and CQC registration

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.

APPENDIX A: DATA BREACH RECORD

Complete for every breach or suspected breach, including those not reported to the ICO. The 72-hour clock starts when we become aware.

Date and time the breach happened (if known)	
Date and time we became aware	
Reported by	
What happened?	
What information was involved, and whose?	
How many people are affected?	
What harm could this cause them?	
Action taken to contain it, and when	
Reportable to the ICO? (yes/no, and why)	
If yes: date and time reported, ICO reference	
Have the people affected been told? When and how?	
CQC notification / safeguarding referral needed?	
Root cause, and what we are changing	
Signed (Registered Manager) and date	

© Supportive Bridge Ltd. Uncontrolled when printed; check you are using the latest version.