## Confidentiality Policy

### Statement

The Bond Board is committed to providing a confidential service to all its service users to protect their interests and right to privacy. The Bond Board believes that individuals have a fundamental right to the confidentiality and privacy of information related to the Bond Board services they receive. Individuals have a right to control access to and disclosure of the information held about them by The Bond Board by giving, withholding or withdrawing consent and to be informed of the implications of doing so. The principles of confidentiality apply to all aspects of the Bond Board service and management. Everyone in the workplace has a legal duty to protect the privacy of information about individuals. This policy aims to support staff in making good decisions about the protection, use and disclosure of service user information.

The Bond Board acknowledges and is committed to complying with all statutory provision related to confidentiality, including: the General Data Protection Regulation 2018; the Human Rights Act 1998, the Children’s Act 1989, 2004 and related Child Protection Policies, the Rehabilitation of Offenders Act 1974, the Sexual Offences Act 2003, the Counter Terrorism Act 2008 and the common law principles of confidentiality.

**GDPR - 6 data protection principles:**

* Lawfulness, fairness and transparency.
* Purpose limitation.
* Data minimisation.
* Accuracy.
* Storage limitation.
* Integrity and **confidentiality**.

**Bond Board policies related to the Confidentiality Policy include the:**

Child Protection Policy, Data Protection Policy, Confidentiality and Conflict of Interest Policy, Adults at Risk Policy.

**Disclosure of service user information**

Disclosure of a service user’s information to a third party will only be appropriate when:

• The service user has given his or her express consent, or

• There is a lawful basis or statutory requirement to use or disclose the information, or

• The balance of public and private interests favours disclosure. In such situations there must be a substantial public interest favouring disclosure which outweighs both the private interests of the individual and the public interest in safeguarding confidentiality.

**All decisions about disclosure of a service user’s information without consent and/or prior notice can only be made by Operational Managers, members of the Senior Leadership Team and/or The Board of Trustees.**

Where a statute, court or tribunal imposes a requirement to disclose information, care will be taken only to disclose the information required to comply with and fulfil the purpose of the law. In all cases of discretionary disclosure in the public interest, an Operational Manager, Senior Leadership Team or the Chief Executive Officer will consider whether the release of information to protect the interests of the service user or a third party exceptionally prevails, both over the duty of confidence owed to the service user/third party.

### Definition of Confidentiality

The Bond Board understands confidentiality to mean that no information regarding a service user will be given directly or indirectly to any third party without prior notice and/or the consent of the service user. Any exemption from this position is laid out below under breaches of confidentiality.

Since service users’ approach for assistance is to the organisation rather than to an individual worker, discussion of particular cases within The Bond Board does not constitute passing details to a third party. This approach is a way for workers to gain support and guidance in their work and should be used with sensitivity.

The Bond Board will not confirm the presence of the service user in offices or his or her use of the service without express consent. Any exemption from this will be laid out below under breaches of confidentiality.

**Confidentiality and Data Security**

Each service user’s right to privacy and employees’ duty of confidentiality exist regardless of the form in which information is held or communicated, for example, verbally, electronic records, paper records, photographs and videos.

The Practical steps all staff and volunteers must take to ensure confidentiality and data security include:

In the office:

* Whenever possible, all information relating to service users will be kept in locked filing cabinets or drawers at the end of each working day. This includes notebooks, copies of correspondence and any other sources of information. You should take care to ensure that no identifying information about service users is visible when people from outside the organisation visit the offices, for example, by leaving printing on the photocopier, or by not locking a computer screen when away from your desk.
* Notes and other records containing personal data which are not to be kept in a secure file or online and are not required to be kept, should be shredded when no longer needed.

**Phone:**

When conducting Bond Board business on the phone and particularly when discussing personal data, staff and volunteers must have regard to Data Protection and confidentiality at all times, including when using a mobile phone outside of the office environment:

* Make sure you are not overheard by any unauthorised person, e.g. a service user in reception.
* Check that you are speaking to the right person before disclosing any personal data.
* When receiving telephone enquiries, only disclose personal data we hold on our systems if you have checked the caller’s identity and made sure that there is a lawful basis for disclosing the information. If you are unsure, make further checks first and ring the caller back. If necessary, ask the caller to put their request in writing and seek advice from a line manager.

**Sending personal data by post**:

* Only use post to send documents which contain personal data if absolutely necessary and you are assured it will reach the intended recipient without interception.
* Ensure adequate postage stamps are attached.
* Ensure the envelope is fastened securely.
* If a postal item is returned undelivered-update records immediately to ensure no correspondence is sent to that address in the future.
* If a postal item is returned undelivered and has been opened, report this to your Line Manager as a potential data breach, in line with the Data Protection Policy.

Further information about Data Security can also be found in the Bond Board’s Data Protection, Working from home, I.T usage and Mobile Phone policies.

**Monitoring and statistics**

The Bond Board is committed to the effective statistical recording of services. It is also required to provide reports to funders to evidence the outcomes of the services it has provided. Where the Bond Board proposes to use or disclose information about service users for monitoring/reporting purposes, the express consent of that service user will be sought, unless the information is in a wholly unidentifiable form.

All staff are responsible for ensuring that information used for monitoring/reporting on service delivery is produced in an anonymous form and does not identify individuals.

**Data Retention**

The Bond Board will keep all service records in accordance with the timescales specified in the Data Protection Policy. After this time records will be destroyed.

### Consent

It is the responsibility of staff to ensure that express consent is obtained from service users before The Bond Board takes any action on their behalf or shares a person’s personal data outside of the Bond Board. Where this action necessitates the completion of a consent form, a copy of this should be kept on file and noted on any relevant IT systems which record consent, such as Lamplight. Services users should be advised of their right to withdraw consent at any time, any consequences of doing so and be directed to the Privacy Notice which outlines their rights in respect of Data Protection.

Staff must be aware that consent from the individual must be specific to the reason you have asked for it. For example, a service user or landlord may have given consent for you to contact to inform them above Bond Board events or to send them a newsletter in the post. This does not mean they have given their specific consent for other uses of their data, such sharing it with a third party organisation.

Staff must be aware that consent is gained from an individual about their personal data. This is particularly relevant when working with a couple or those with non-dependants as consent for each individual must be obtained and recorded. Consent in respect of children’s data, must be obtained from their parent or legal guardian.

Where a service user refuses to consent to a specific disclosure or withdraws consent, this should be clearly documented in their case file and any appropriate Bond Board I.T systems that are being used to record client data.

Where it is planned to involve staff from other agencies this should first be discussed with the service user and their explicit consent sought. When other agencies request information about service users, staff should seek the consent of the service user before disclosing any information or confirming the service user is known to The Bond Board.

If a service user refuses to consent to disclosure of personal information, the information cannot be disclosed, unless, exceptionally, a justification other than consent exists. Staff should discuss with the service user why disclosure may be in the service user’s best interests and the potential disadvantages that may arise without it. **Unless there is an overriding public interest or legal justification (to be determined by the Operational Managers, Senior Leadership Team or Chief Executive Officer information should not be disclosed on a “best interests” basis where an adult with capacity refuses to consent to disclosure.**

In any circumstance where an employee believes an adult is incapable of giving or withholding consent due to lack of mental capacity and an employee believes they are at risk, for example a victim of neglect or of emotional or physical abuse or at risk of suicide, any breach of confidentiality must be discussed in advance with an Operational Manager, Senior Leadership Team or the Chief Executive Officer.

An Operational Manager, Senior Leadership Team or the Chief Executive Officer will also make all decisions in respect of breaching confidentiality where an employee has concerns about the safety or protection of a child and where it is impracticable or inappropriate to obtain consent from the person with parental responsibility.

Members of staff will ensure they record on the case file acceptable methods of contacting service users, e.g. by phone or letter, home or work etc., to avoid breaching confidentiality.

Information will be displayed in publicly accessible areas of the Rochdale office advising all clients of the existence of this policy and their right to request a copy of it, along with information about our Service User Privacy Notice in respect of Data Protection rights.

At the point of access to specific Bond Board services, service users (and anyone else whose personal data The Bond Board processes), will be provided with specific written information relevant to that service, which explains:

■ what kind of information is being recorded and retained

■ the purposes for which the information is being recorded and retained

■ what protections are in place to ensure non-disclosure of their information

■ what kinds of information sharing will usually occur, with whom and for what purpose, for example any inter-agency information sharing protocols or reporting obligations to funders.

■ the choices available to them about how their information may be used and disclosed

■ their rights to access and where necessary to correct the information held about them within their records.

■ the mechanism for withholding or withdrawing consent in the future,

■ how to raise any concerns they may have about possible uses or potential misuse of their information.

■How to access a privacy notice which contains further information about their rights in respect of their personal data.

Bond Board employees should always be mindful about the location in which they have discussions with or about service users, so that any private, sensitive or confidential information is not overheard or inadvertently accessible to others. Any means of communication of confidential information (for example, telephone or email) should also ensure the privacy of the service user.

Employees should only seek information about a service user’s personal information from another Bond Board employee when there is a legitimate need to access that information and the person has the authority to disclose it. Service user information should not be shared more widely than is strictly necessary.

Employees should be mindful of checking the identity of any person requesting information, including someone claiming to be a member of another service/organisation and the clients consent status, before releasing any service user information.

Employees working in outreach locations, at home or travelling have a duty to ensure that confidential information is safeguarded at all times. This includes not allowing the details on the front of or in a casefile to be seen by anyone outside of the Bond Board and keeping information in a secure, lockable location when not in use.

The confidential nature of a service user’s information continues to apply after the death of that service user. Where a competent service user has made an explicit request before his or her death that their confidence be maintained, then the service user’s request will be respected.

Further guidance for staff about protecting service user confidentiality is contained with the Bond Board’s Data Protection Policy.

**Service user access to own records**

The Bond Board is fully committed to allowing service users the right of access to their case records and to any other information held about them by The Bond Board. No charge will be made in respect of providing service users with information held about them. Any information which exists in the record about third parties (other than relevant professionals) will not be disclosed without the consent of the third party. Guidance about handling requests for access to case records and other data subject rights is contained within the Bond Board’s Data Protection policy.

### Breaches of Confidentiality

The Bond Board recognises that occasions may arise when employees feel it is appropriate to breach confidentiality. A non-exhaustive list of circumstances of when this situation may arise include the following:

* Child protection
* Making a referral for a service user with a conviction for sexual offences against children
* Protection of vulnerable adults
* Prevention of harm to service user or third parties.
* Prevention of terrorism and other breaches of the law.
* Prevention, detection or prosecution of a serious crime.
* The Chief Executive Officer may also decide to notify the Disclosure and Barring Service (DBS) when a staff member or Volunteer is dismissed for gross misconduct, and/or theft. In these circumstances, the Senior Leadership Team and The Chief Executive Officer must consider the risk of harm to vulnerable adults and children should concerns arising during their role at The Bond Board not be disclosed/made known to other potential employers.

The member of staff will raise any proposed breach of confidentiality with their Operational Manager before any breach is made. Operational Managers should contact a member of the Senior Leadership Team. The issues involved in the case will be discussed with the purpose of determining whether there is a:

■ A statutory requirement to use or disclose the information, or;

■ The balance of public and private interests favours disclosure. In such situations there must be a substantial public interest favouring disclosure which outweighs both the private interests of the individual and the public interest in safeguarding confidentiality.

Where there is no statutory duty to breach confidentiality, the Operational Managers, Senior Leadership Team or Chief Executive will consider:

• Data Protection regulations

• The nature and extent of the proposed disclosure

• The importance of the interest that is at risk without disclosure. For example disclosure might be more easily justified where it is in a person’s vital interests, such as a life or death situation.

• The likelihood of the harm occurring in the individual case. For example, disclosure might be justified where there is a high likelihood of harm to the life of another, but not necessarily justified where there is a low likelihood of harm.

• The imminence of the harm. For example, disclosure might be justified where protection of the service user or third party requires immediate action, but not where there is no more than a possibility that at some future point the service user might pose a threat to self or another.

• The existence of an appropriate person to whom disclosure can be considered.

• The necessity of the disclosure to avert the harm, that is, where there is no reasonable possibility of averting the harm without disclosure.

• The likelihood that disclosure can avert the harm, which requires satisfaction that the harm to the service user, third party or to the public interest is sufficiently likely to be averted by disclosure.

Written notes of the discussion will be taken by the Manager leading on the breach. The Senior Leadership Team, Chief Executive Officer or the Chair of Trustees is responsible for making a decision on whether confidentiality is to be breached. Their decision is final and cannot be overridden by the employee. If confidentiality is to be breached the following procedure will be implemented:

* The Senior Leadership Team, Chief Executive Officer will contact the Chair of the Board of Trustees in the first instance. The Chief Officer will brief the Chair on the full facts of the case. The Chief Officer will seek authorisation to breach confidentiality from the Chair or Member of the Board of Trustees.
* If the Chair of the Board of Trustees agrees to breach confidentiality, a full written report will be made and any action agreed undertaken. The Chief Executive Officer or Senior Leadership Team is responsible for ensuring that all necessary action arising from the decision is completed.
* The Chief Executive Officer, Senior Leadership Team or Chair of the Board of Trustees will make a decision as to whether it is appropriate to disclose the breach of confidentiality to the service user even though the disclosure does not need their consent to be justified. Consideration will include any legal obligations, the potential risks involved of exposing the breach and The Bond Board’s commitment to maintaining relationships of transparency and trust with their service users.
* The Chair of the Board of Trustees decision is final.
* The Chief Executive Officer or Senior Leadership Team is responsible for maintaining a file containing relevant paperwork as outlined above in relation to such issues of confidentiality.

Any breaches of confidentiality that do not meet these circumstances, or where this procedure is not followed will potentially be regarded as serious misconduct and as such may result in disciplinary action. All employees are obligated to raise and report any concerns they have about unauthorised breaches of confidentiality to the Senior Leadership Team or Chief Executive Officer.

### Monitoring the Policy

All Board of Trustees, staff members and Volunteers will receive a copy of the Confidentiality Policy. New Members of staff and Volunteers will be given a copy of the Confidentiality Policy and will be introduced to the Confidentiality Policy as part of their induction. The procedure will be reviewed every three years or sooner in the event of any incidents involving a breach.