Confidentiality Policy

Policy Title:	**Confidentiality**
Policy Number:	B108
Version Number:	2
Ratified By:	B3, Board Of Trustees
Date Of Issue:	March 2014
Date Of Review:	May 2016
Cross References:	Safeguarding Adults Policy Safeguarding Children Policy
Additions/Amendments:	

Confidentiality Policy

1. Introduction

1.1. B3 recognises the importance of confidentiality. It is essential to the effective running of the B3 services. B3 recognises the right of individuals in having their personal information protected and as such operates strict practices to ensure that personal information is held securely and shared appropriately.

1.2. This policy sets out many of the practices that must be adhered to in order that individual's personal information is secured.

1.3. This policy is intended to ensure that all B3's staff and volunteers understand the responsibilities they have for ensuring the confidentiality of all sensitive information and to know what to do when there is a need to breach confidentiality. This policy is written within the framework of the Data Protection Act 1998 and follows the guidelines laid out within the NHS Information Governance Toolkit.

1.4. Throughout this document, the term 'staff' applies to permanent, temporary, sessional and volunteer workers.

1.5. Service users is anyone who approaches or engages in the service for help, advice and information, along with those engaged in any of the Brent partnership services.

2. Responsibilities

2.1. It is the responsibility of all staff, volunteers, students and contracted staff working on behalf of B3 to ensure that they maintain high standards of practice that in turn results in the maintenance of confidentiality and that they follow the processes outlined in this policy.

2.2. It is the responsibility of all staff, volunteers, students and contracted staff working with services users on behalf of B3 to ensure that service users they are working with fully understand both consent to treatment and consent to information sharing. Staff members must also ensure that individuals are able to give this consent.

2.3. It is the responsibility of the service manager to ensure that staff and volunteers within their services maintain appropriate confidentiality procedures in line with this policy and national guidance and to ensure their service has appropriate accommodation, equipment and protocols in place to achieve this. This will include an appropriate consent form similar to that in Appendix A.

2.4. It is the role of the organisation's service manager to ensure that the roles afforded to them outlined in this policy are fulfilled.

3. Monitoring & Evaluation

3.1. At a service level this policy will be monitored by service managers through case file audits and B3's normal performance management and supervision processes.

3.2. This policy will be monitored by B3's service manager and/or Board of Trustees.

3.3. In addition all issues resulting in breaches of confidentiality or data loss will be reported through B3's incident reporting process and this in turn will be reported to the Board of Trustees and service manager where a strategic view will be taken.

4. Confidentiality

4.1. Service users have a right to expect that information about them will be held in confidence by workers. This policy sets out the principles of confidentiality and respect for service users privacy that all B3 employees and volunteers are expected to understand and follow.

4.2. When service users approach B3 for support it must be remembered that they are approaching a service and it is important to acknowledge that identifiable information is and will be shared within the B3 care team associated with that individual in order to maintain appropriate care. This must be explained to individuals on initial entry to the service and written consent obtained from each service user prior to recording and storing any personal or sensitive information. This is discussed further in section ten of this document.

5. Sharing Information With Other Organisations

5.1. B3 is in principle committed to partnership and joint work in the interest of service user, staff and wider community safety as well as to ensure the best support and outcomes are achieved for service users.

5.2. Service users will be advised of this at initial contact. Any differences between B3's confidentiality policy and that of a partner agency will be discussed with the service manager and agreement to an acceptable local policy made.

5.3. Any problems arising from partnership work must be discussed as soon as possible so that resolution can be sought.

6. Service Users Rights And Expectations

6.1. Service users have the right to expect to be treated with discretion and sensitivity when accessing B3's services. This policy aims to provide service users, staff and other agencies with clear guidelines which fit within a legislative framework.

6.2. This policy is based on the principle that the service users interests, wishes and rights are of fundamental importance and draws upon guidance produced and published by Public Health England — please see the website for the full toolkit (www.nta.nhs.uk). A service user who uses B3 services can be confident that:

6.2.1. Information given by the service user will only be used for the purpose for which it was disclosed and will not be shared with anyone outside B3 without the consent of the client, except as stated below (see 'Limits of confidentiality' below)

6.2.2. All records will be securely stored (refer to Security and Transportation of Confidential Information and Records Management policies)

6.2.3. Information received from the service user will be treated as confidential to B3. Where B3 wishes, or has been requested, to disclose information to a third party then the full and informed consent of the service user will be requested. The service user has the right to withhold consent either with regard to a specific piece of information or a specific agency. If consent is withheld, information will not be shared unless there are exceptional circumstances (see below)

6.2.4. In some cases service users will provide information in the expectation that it will be shared outside B3. It will still be made clear to the service user what information will be passed on and to whom

6.2.5. Service users will be asked to sign a consent form detailing with whom information can be shared and what information will be shared. This consent also outlines for what purposes the information will be used for. Please see the Appendixes for example consent forms.

6.2.6. B3 may use service user information for research purposes. In these cases, client's identities will be protected at all times, unless specific consent to participate openly in a research programme is gained from the service user.

7. Limits Of Confidentiality

7.1. Information about service users is confidential to B3 as a whole and not to individual workers.

7.2. B3 does not operate a policy of absolute confidentiality. The following circumstances legally override the need for confidentiality. Workers will consult their line management before breaching confidentiality.

7.2.1. When there is concern that a user of the service is putting themselves or a third party/individual at risk (especially when that individual is a child).

7.2.2. Note that suspected child abuse must always be viewed as sufficient reason to breach confidentiality and the decision whether or not to disclose must always be taken in the best interests of the child. "Significant harm" is determined on the basis of professional judgement, and means impairment of a child's health or development (physical, intellectual, emotional, social or behavioural). It includes sexual abuse and forms of behaviour that hinder the ability of a child to thrive. For further details please refer to the Children's Act 2004, B3's Safeguarding Children & Safeguarding Adults policy which outlines the process and procedure in such situations.

7.2.3. When instructed by the courts, or in certain limited circumstances by the police acting on the authority of the courts, to reveal information. In cases where the service is not sure whether to break confidentiality, they should contact service manager to seek advice on procedure and obligations of the service.

7.2.4. Where B3 or an individual worker has been instructed to do so by a court by means of a witness or subpoena, or where the police ask a direct question under an order from a circuit judge (e.g., coroners court).

7.2.5. Where there is a statutory obligation to disclose information, for example to the Serious Fraud Office or in relation to the Drug Trafficking Offences Act (please refer to B3's data protection lead or the Government's Information Commissioner's Office).

7.2.6. If the service user gives specific details about a serious crime which has been committed or is to be committed (murder, rape, serious offence against another person, etc.).

7.2.7. In prisons, where there is a threat to prison security.

7.3. Examples of other circumstances in which B3 will consider breaching confidentiality on the basis of ethical obligation rather than legal rules are (please note that this is not an exhaustive list):

7.3.1. A medical emergency where information will be given to medical staff.

7.3.2. Where a client's behaviour has resulted in notifying or calling the police. For example, refusing to leave the premises. In such circumstances, all efforts should be made to protection other service users' anonymity.

7.3.3. If the service user has threatened or seems likely to do serious harm to him/herself.

7.4. B3 has a duty to consider breaching confidentiality where a service user continues to drive a vehicle for non-commercial purposes (such as his/her own car) without disclosing his/her drug/alcohol use to DVLA (Driving Vehicle Licensing Authority). To the DVLA and/or the service user's employer in the following three scenarios:

7.4.1. If s/he repeatedly fails to provide proof of disclosing to the DVLA, B3 staff are expected to breach confidentiality (as per the guidance in paragraph 8.3 of this policy) and inform the DVLA that the service user is in treatment for Drug and/or Alcohol misuse. The medical director could advise on the precise wording in each case.

7.4.2. A service user who continues to operate as a professional driver (in a taxi, bus, train, heavy good vehicles and such like) should be immediately informing both the DVLA and his/her employers that s/he is in treatment for drug/alcohol misuse.

If the professional driver has not provided proof of disclosure by the second appointment with our service, B3 staff are expected to breach confidentiality (as per the guidance in paragraph 8.3 of this policy). The B3 staff duty to disclose remains if the service user drops out of

treatment and does not return for a second appointment. The medical director could advise on the precise wording in each case.

7.4.3. A service user who is professionally involved with vulnerable people. Vulnerable people in this context include, but are not limited to: children; adults with physical or psychiatric problems; older adults; anyone needing provision of treatment and care. Example of professional service users referred to in this paragraph are: doctors, nurses, paramedics, nannies, carers of old and vulnerable people, teachers and others.

The service users professionally involved with vulnerable people have to immediately disclose their drug and alcohol use to their employers, if proof of disclosure has not been provided by the second visit with our service, B3 workers are expected to breach confidentiality (as per the guidance in paragraph 8.3 of this policy) and notify their employers of their drug/alcohol misuse.

7.5. All records kept by B3 could be used in a court case, and could be an essential element of either prosecution or defence's evidence in court.

7.6. Documents relating to interventions made with a service user enjoy a degree of protection under the Police and Criminal Evidence Act 1984 (PACE) and current Codes of Practice (please see http://police.homeoffice.gov.uk/operational-policing/powers-pace-codes/pace-code-intro/ for further details). PACE concerns the protection of "personal records" and defines them thus:

7.6.1. Documentary and other records concerning an individual (whether living or dead) who can be identified from them, and relating:

- To his/her physical or mental health;
- To assistance given to him/her;
- To assistance given to him/her, for the purpose of his personal welfare, by any voluntary organisation or by any individual who (i) by means of his/her office or occupation has responsibilities for his/her personal welfare; or (ii) by reason of his/her court order, has responsibilities for his/her supervision.

7.7. In cases where the service user has been excluded from a project/service, magistrates cannot issue search warrants for such "excluded" documentation. However warrants can be issued by a circuit judge.

8. Breach Of Confidentiality

8.1. To be read in conjunction with the following polices and procedures:

8.1.1. Safeguarding Children Policy

8.1.2. Safeguarding Adults Policy

8.1.3. Section 5 of this policy — sharing information with partner agencies

8.2. If it appears that confidentiality will have to be breached, the worker must make every effort to discuss the situation with the service user unless it is agreed that this would worsen the situation. Staff should seek advice from their line manager when considering sharing information without the client's permission and where possible the service user should be encouraged to take responsibility for contacting the relevant authorities. (If the service user discloses the required information there will be no need to breach confidentiality.)

8.3. Decisions to breach confidentiality must not be decided by an individual worker, unless it is dangerous to wait, but in conjunction with their line management, who will direct the course of action. Where local line management are not available the decision should be taken in conjunction with senior management. Risk factors must be taken into consideration such as potential harm to the worker or other parties, and plans to reduce the risk must be implemented.

8.4. Any breach will be minimised by restricting the information conveyed to that which is relevant to the immediate situation.

8.4.1. The circumstances will be recorded in the service user file outlining:

- the extent of the disclosure
- to whom it was made and when
- the reason for the disclosure
- who was consulted beforehand
- whether the service user was informed, and if so how and when
- the consequences of the disclosure

8.5. The service user has a right to invoke B3's complaints procedure if they feel their right to confidentiality has not been upheld.

8.6. Service users who wish to complain must be reassured that it will not affect the service offered to them by B3 (Please see Complaints policy for further details).

9. Sharing Information Within The Organisation

9.1. Service user information will be shared between workers within the service or assisting the service, on a need to know basis only. That is the amount of information that needs to be exchanged to provide proper care for the client. Anonymous or pseudo-anonymous data may also be shared with other members of B3 for the purposes of monitoring, evaluation and research this will be made explicit in all service user consent forms (see Appendixes). Again, this is strictly on a need to know basis and in such cases, personal data and contact details should be removed to protect the service users' identity.

9.2. Details of information sharing either within or outside the organisation should always be contained within the information provided to the service user about the service, as well as the consent form itself.

10. Consent To Share Information

10.1. Service users where they are able must give valid consent to disclosure of any confidential information unless outside the limits of confidentiality as detailed in section 7 above.

10.2. B3 services will have arrangements in place for obtaining informed consent in relation to disclosure or sharing of confidential information. Informed consent means that the service user is given the information required to make a decision and is competent to make that decision.

10.3. The giving of consent can only be given if the individual is competent to do so. The legal test for competence is: “first comprehending and retaining information, secondly, believing it and thirdly, weighing it in the balance to arrive at a choice". (Re C 1994)

10.4. B3 services working with young people will have procedures for assessment of competence to consent. Children aged 16 and 17 are presumed in law to be competent to consent unless they do not meet the legal test for competence.

10.5. Competence in the case of an under 16 year old will be considered in relation to Gillick competency and the Fraser guidelines for offering contraceptive advice and treatment without parental consent. Under 16’s may be considered to be competent to consent if:

10.5.1. The young person will understand the professional's advice;

10.5.2. The young person cannot be persuaded to inform their parents;

10.5.3. The young person is likely to begin, or to continue, the behaviour in question with or without treatment;

10.5.4. Unless the young person receives treatment, their physical or mental health, or both, are likely to suffer;

10.5.5. The young person's best interests require them to receive advice or treatment with or without parental consent.

10.6. In all cases it is preferable if parents are involved with the young person’s treatment. However, if using the above guidelines B3 has assessed a young person to be competent to give consent on their own then this cannot be overridden by a parent.

10.7. Where an adult is not competent to consent, then the High Court is empowered to make that decision on their behalf. Where a child is not competent to consent, those with parental responsibility or the High Court may make the decision on their behalf.

11. The Role Of Staff, Students And Volunteers

11.1. Information about service users is confidential to B3 and not individual workers. All workers will understand the Confidentiality Policy and accept responsibility for the security of the information they encounter. However not all workers have

equal access to confidential information, with service user information will being shared on a need to know basis. Confidentiality extends to the worker's knowledge of all service users. Discussion of service users with colleagues will always be purposeful and sensitive.

11.2. Staff training: It is important that all staff have a clear understanding of how the principles of confidentiality are embodied in practice. B3 will take all reasonable and practical steps to prevent the disclosure of confidential information. This will be done through training and instructing staff, and ensuring appropriate administrative arrangements are made. Appropriate security will be provided through IT, with B3 staff briefed on its use and the IT. Training will also be delivered to all staff on the Data Protection Act 1998, its principles and consequences for B3 through familiarisation with policies and line management.

11.3. Workers' responsibilities in relation to confidentiality: It is the responsibility of the worker to ensure service users understand the confidentiality procedures which apply at all stages of their contact with B3. All new staff will be required to sign a contract, which includes their responsibility to adhere to the Confidentiality policy and other relevant policies. Breaching the contract may lead to disciplinary action under the disciplinary procedure (Please see Disciplinary policy).

12. Specific Situations

12.1. Service users referred by other organisations: The extent of information to be shared with the referrer, if any, will be discussed with the service user at the earliest opportunity. If the service user consents, it will be necessary to ascertain the nature of the information shared — please refer to Section 2 of this policy.

12.2. Service users who self-refer: Information will not usually be shared with other agencies, unless an appropriate information-sharing protocol is established between partners. If it becomes necessary to share service user information, every attempt will be made to ensure the full and informed consent of the client.

12.3. When an enquiry is received from a partner, relative or friend: No information will be given without the client's permission unless the limits of confidentiality noted above apply. When such requests are made it is vital that staff remember that this may be a very emotive subject for family and friends and as such sensitivity must be used when declining information.

12.4. Service users who request contact with other organisations: When the service user has given consent to information being shared, it must be clarified as to how much information is shared and with whom. The worker has an obligation to ensure that the service user is clear about the consequences of disclosure.

12.5. Service user enquiries: A staff member or B3 representative will always take incoming calls. Information will not be given without prior written consent from the service user or in agreed circumstances with specific organisations or individuals. Consideration should be given to an appropriate response should the caller be enquiring about a service user B3 does not have permission to discuss with them. The caller's identity and telephone number will be

established by calling them back after having checked the number. Telephone calls will be taken in a place where non — staff members cannot overhear conversations — if this is not physically possible, consideration should be given to the content of the conversation. B3 staff may ask for non-urgent requests for information to be put in writing, e.g., details of drug related deaths.

13. Employment Practice Relating To This Policy

13.1. B3's confidentiality policy is fundamental to the effective and successful running of its services. It is therefore essential that all staff fully understand and support the policy. They will be involved in consultation and review of the policy.

13.2. B3 will ensure that:

13.2.1. Staff members are properly qualified, trained and competent to receive confidential information and deal with the issues raised.

13.2.2. Staff members induction involves familiarisation with B3's Confidentiality policy.

13.2.3. Staff members receive training and support in its implementation throughout their employment with B3.

13.3. This will involve instruction in areas such as:

13.3.1. Details of the policy and data protection requirements in accordance with the Data Protection Act 1998.

13.3.2. Appropriate communication of the policy to service users.

13.3.3. Safe storage and archiving of data both on paper and electronic (see Records Management policy).

13.3.4. Procedures for note-taking (also see Records Management policy).

13.3.5. Dealing with enquiries (telephone or otherwise).

13.3.6. Procedure for Breach of Confidentiality

13.4. Staff must not discuss service users outside B3 or partnership services, or otherwise act in a manner which threatens a client's confidentiality.

14. Notes And Records

14.1. Recording and storage of notes: All notes and records should be written, stored and transported in line with B3's Case Management policy, Records Management policy and the Security and Transportation of Confidential Information policy.

14.2. Note-keeping: The scope and extent of the information to be recorded will be discussed with the service user at registration;

14.2.1. Records must be accurate, non-judgmental, factual and objective.

14.2.2. Errors will be crossed out with a single line; no correction fluid to be used.

14.3. In addition, personal data should be adequate, relevant and not excessive for the purpose for which its held and not kept for longer than is necessary (see guidance on the retention and destruction of records/notes within the Data Protection Act 1998).

15. Data Protection Principles

15.1. The principles laid out in this policy are in line with the data protection act 1998 but is essential B3 staff are familiar with and work in line with the data protection act and as such a summary of the act is detailed below:

Data Protection Act 1998 Principles 1 – 8

First principle
Personal data shall be processed fairly and lawfully.

Second principle
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Third principle
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth principle
Personal data shall be accurate and, where necessary, kept up-to-date.

Fifth principle
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth principle
Personal data shall be processed in accordance with the rights of the data subjects under this Act.

Seventh principle
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth principle
Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

15.2. B3 staff should refer to the Information Commissioner's Office website for further guidance on the Data Protection Act 1998 and its principles — http://www.ico.gov.uk/

16. Service User Access To Files

16.1. Service users have right of access to their own records in accordance with:

16.1.1. The Data Protection Act 1998

16.1.2. The Access to Personal Files Act 1988

16.1.3. The Access to Health Records 1990

16.1.4. Freedom of Information Act 2005 – this only applies to statutory services, however, please refer to local service contracts to ascertain agreed procedures should a Freedom of Information request arise.

Requests for information should be processed in accordance with the Information Requests Procedure.

16.2. This legislation permits a service user's rights to be restricted in the following situations:

16.2.1. Where information has been provided by a third party and it is considered in the best interests of the service user not to share the information provided. The decision to restrict information will be made by the service manager or Board of Trustees.

17. Use Of Information For Planning, Research And Publicity

17.1. Information used for monitoring and planning purposes by B3 will be presented statistically, or in aggregated form. This will ensure individuals are not identifiable. Information sheets and consent forms will contain details of use of the service user information.

17.2. Explicit consent from the service user will be obtained before information about them is used for publication. His/her anonymity will be preserved.

17.3. Recognisable photographic images of service users will not be used in any B3 publicity. Explicit consent will be gained before service users are subject to research or have information about them used in publicity material.

17.4. Any approach to the service user via B3, by researchers or media representatives will be treated with caution. B3 will not disclose personal details concerning the client. B3 will undertake to brief the service user fully regarding the purpose of such an approach to allow the service user to decide whether she/he is prepared to be the subject of inquiry.

17.5. B3 will warn the service user that neither B3 nor the service user may have control over the final material and that there is the possibility that confidentiality may be breached.

18. Safe Havens

18.1. Most B3 services work closely or in partnership with NHS services and as such staff and services should be familiar with the term "Safe Haven". The Term "Safe Haven" was originally implemented to support contracting procedures. Today it is a term recognised throughout the NHS to describe the administrative arrangements to safeguard the confidential transfer of service user identifiable information between organisations or sites using the following format:

18.1.1. Fax Machines

18.1.2. Post/Email/Telephones/Answer Phones

18.1.3. Computer Systems/Electronic Media, Manual Records and Books

18.1.4. White and Notice Boards

18.2. The objective in safe havens is to ensure that the use of service user information is handled in the most secure manner and by authorised personnel only on a need to know basis. When information is disclosed by a designated safe-haven point to an equivalent point in another organisation, staff can be confident that agreed protocols would govern the use of the information from that point on.

18.3. B3's policies and procedures are in line with the principle of safe havens and as such if good practice is followed there is no reason why B3 services should not be considered safe havens. Services may wish to make locally agreed protocols with NHS partners to cement this point.

19. Sample Of Consent (Appendix A)

19.1. "You will maintain service users confidentiality under all circumstances. You accept that any breach of these rules will result in the termination of your role as a B3 member. However, there are certain circumstances under which it is necessary to break confidentiality.

19.1.1. If you believe that there is a risk of serious harm to yourself, the service user or to another, especially children.

19.1.2. If a service user admits to be about to commit a serious offence.

19.1.3. If a service user admits to being involved in a serious crime which has not been reported to the police.

19.1.4. If required to do so by the police or the courts, upon receipt of the appropriate paperwork from the authorities concerned.

19.1.5. When a service user requires medical attention and is not in a position to give informed consent".

19.2. You will keep the confidence of all the B3 members and BSAFE volunteers as some may be service users and/or volunteers at other services. If you also work for another service provider you will adhere to their confidentiality policy with regard to both our service users and volunteers and vice versa.

20. Photo Consent Form (Appendix B)

B3 produces a range of materials to tell people about our service. From time to time we take photographic images (moving and still) of people and events to illustrate our work.

By completing this form, you give us full permission to use these images in our media applications, which reasonably promotes or advertises B3's aims. (This may include our printed publications; adverts; audiovisual and electronic materials; media work; and any other media we may use in the future.) The images will not be used for any other purpose.

The copyright of any material we generate is the property of B3 Brent Service User Council.

First Name	Last Name	
Address		
	Postcode	
Telphone	Email	
Can we reference your full name?	☐ Yes	☐ No
Please state here if there are any ways in which you do not want us to use photo(s) of you:		
Signed	Date	

Thank you

21. Supervision Confidentiality Agreement (Appendix D)

This agreement MUST be signed before commencing supervision. It provides volunteers and supervisors with a clear understanding of where the boundaries of confidentiality lie, so as to protect and maintain a safe, effective relationship.

CONFIDENTIALITY:

Discussions will only be shared with others by mutual consent. Unless there is a clear responsibility to share information with the service manager which affects the management and dynamics of the team e.g. issues relating to disciplinary, capability, grievance or sickness nature, or quality of work.

GROUNDRULES:

- Confidentiality: If issues are raised in supervision which concerns the supervisor i.e. unsafe or unethical practice by the volunteer or issues which concern harm to self or others (as outlined in the confidentiality policy and Codes Of Conducts).
- Openness/honesty.
- Agree no Gossip.
- Using feedback to learn.

ARRANGEMENTS AGREED FOR SUPERVISION:

a) Frequency: Once a month
b) Length: 1 hour
c) Location: BSAFE
d) Agenda: As outlined in the following 'supervision notes'.
e) Records: The supervisor will maintain the written notes and keep them in the B3 office. All notes will be signed as agreed records at the end of a session or beginning of the next. N.B. It is the volunteer's responsibility to record any agreed action points.
f) Any areas of concern that are not satisfactorily resolved will be referred to the service manager.

Volunteer name (print):

Volunteer signature: **Date:**

Supervisor name (print):

Supervisor signature: **Date:**
