THE BOLTON WOODS CENTRE

GDPR AND DATA PROTECTION POLICY

REVIEWED 01/07/2024

Contents **Page**

The Bolton Woods Centre

GDPR and Data Protection Policy

1. Introduction

The Bolton Woods Centre (BWC), is located in the Bolton Woods neighbourhood, supporting residents of the immediate and wider locality to access a needs- based, inclusive offer appropriate for everyone.

2. Policy statement

BWC is committed to the protection of all personal and sensitive data for which it holds responsibility. As the Data Controller, handling of such data will be used and kept in line with the Data Protection Act (1998) and as of 25th May 2018, the General Data Protection Regulation ('GDPR'). We respect that certain information gathered about an individual must be kept confidential and as such, appropriate steps will be taken to ensure the privacy of all data and that it is taken seriously.

BWC Board of Trustees intend to comply fully with the requirements and principles of the Data Protection Act (DPA) and the new GDPR legislation. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities, as outlined by the guidelines covered in this policy.

This policy refers to the protection of the privacy of staff, volunteers, job applicants, trustees, service users and any other person about whom The Bolton Woods Centre holds personal information of a formal or informal nature.

3. Personal and sensitive data

All data within BWC control shall be identified as personal, sensitive or both, to ensure that it is handled in compliance with legal requirements and that access to it does not breach the rights of the individuals to whom it relates. We only process the personal data we need in order to provide our service.

Personal data is defined by DPA as 'basic information that can be used to identify an individual". This includes names, date of birth, addresses, phone numbers, email address, bank details and IP addresses. It can also include any information regarding an individual's personal attributes or identifying descriptions. Sensitive data is referred to as confidential information, either verbal or written, which is not meant for public or general knowledge. This includes information regarding an individual's health, financial circumstances, criminal records, racial/ethnic origin, sexuality and political views. BWC will only process such information if necessary.

3.1. Information relating to the community.

BWC collects personal information from families, residents and the public, ensuring that relevant data is held safe, for purposes of funding requirements, promotion and publicity.

This includes:

- Full names of attendees
- Their date of birth as proof of age
- Home address
- Guardian, carer details as appropriate
- Ethnicity
- The school that they attend (children and young people)
- Any information that may affect their ability to fully participate, past and present health conditions
- Media consent forms to include photographic and video evidence of sessions, for publicity purposes.

3.2. Information relating to staff

BWC holds information about employees to do with their working life and to fulfil its responsibilities as an employer. Personal information is also held about trustees. Data held includes:

- Information relating to recruitment and selection such as application forms; references; proof of eligibility to work in the UK; where relevant, unspent criminal records and/or the outcome of Disclosure and Barring investigations.
- Personal details of employees' home address, phone number and next of kin.
- Information necessary for payment or salaries; bank details, national insurance number, details of deductions e.g. pension.
- Academic and vocational qualifications and experience.
- Notes of probationary periods, annual reviews and supervisions.
- Sick notes and medical assessments, including information relating to disabilities.
- Absence records, including sickness, compassionate leave and unauthorised absences.
- Time sheets and holiday sheets.
- Details of grievance and disciplinary proceedings including current warnings.
- Reference requests and responses.

BWC understands its duty to safeguard data collected by all means possible and to notify staff about what is kept and why, along with information about how data can be accessed and by whom. For further information on where personal and sensitive data is stored please see page 6.

4. Privacy notices

BWC will request consent from parents and carers of anyone under the age of 16. A Privacy notice has been attached to all consent forms to ensure that those supplying personal data understand why, what, how and with whom information will, or could be shared. BWC consent forms clearly state that information shared will never include CYP's names, therefore making it unidentifiable. There may be circumstances where BWC is required, either by law or in the best interests of CYP, to pass information onto external authorities. This may be due to a safeguarding concern or a health-related incident. This is stated clearly on all privacy notices.

Images of staff, CYP and families may be captured at appropriate times and for many reasons. This includes evidencing the work that we do, for consultation and for archive reasons. BWC also uses

personal data, such as first names and photographs, for publishing purposes. This includes on newsletters, annual reports, our website and leaflets. Consent forms will be published in such a way to allow anyone to opt out, details of which will be held in a safe place, and shared across core staff

BWC will never publish home or personal contact details.

5. Recording and managing information

In implementing this policy, BWC will follow the eight data protection principles of good information handling in respect of personal information. These are:

- Data will be processed fairly and lawfully.
- Data will only be used for purposes detailed in this policy.
- Ensure that all data processed is adequate, relevant and not excessive.
- Data will be accurate and up to date.
- Data will not be kept longer than necessary.
- Data will be processed in accordance with the data subject's rights.
- Data will be held securely.
- Ensure that data is not transferred to other countries without adequate protection.

BWC is committed to ensure data integrity by the following methods:

- **Data accuracy**
  Data held will be as accurate and up to date as is reasonably possible. If a CYP's personal data were to change then we ask that they update us as soon as possible. This is stated clearly on all consent forms and staff have regular conversations with CYP and parents to ensure that all data is accurate. Personal data regarding staff members will also be reviewed annually to ensure that information is accurate.
  If a CYP or parent were to challenge the accuracy of their data, BWC will immediately mark all records regarding the individual as potentially inaccurate. This could include the questioning of a young person's age or identifying the correct contact number of a parent or carer. It is important that all personal and sensitive data held by BWC is correct prior to sessions.

- **Data adequacy and relevance**
  All personal and sensitive data will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. To ensure compliance with this principle, BWC will check records regularly for missing, irrelevant or seemingly excessive information. This includes an annual review of all consent forms to ensure that CYP details are correct. Nominated staff shall be responsible for ensuring that all data referring to CYP is kept up to date by contacting regular session users on a yearly basis.
  Employees at BWC are asked to notify the organisation of changes in personal details as soon as possible.

- **Length of time**
  It is BWC s duty to ensure that obsolete data is properly erased. Data held by BWC will be retained for no more than 7 years, except in circumstances such as funding requirements, child protection matters and health and safety incidents. If BWC deems it necessary to keep

this information, such information will be stored on a password protected computer and not in physical form. Access should then be restricted and only accessed by those appropriate. It is the data manager's responsibility to destroy all consent forms of a young person who has reached the age of 18 or has been un-attending sessions for over two years.
Secure means must be used to destroy consent forms, i.e. shredding or deleting files.

6. Location of information and data

Hard copy data, records and personal information are stored out of sight and in a locked office. BWC store all confidential records referring to members of staff in a locked draw. All financial records about the organisation are stored in a locked office, filed in date order. Care is taken to ensure that sick notes, absence records and other health-related information is stored securely and that access is limited. Only senior members of staff will have access to this information and no other personnel will be allowed access to such data without prior consent given by the manager.

Confidential records relating to children and young people will be kept separate from staff records and in a locked draw, filed in the form of consent forms and in alphabetical order. Senior members of staff will determine who is given access to this information and at what times. Records relating to children and young people should not be stored indefinitely on a PC; however when necessary, confidential records will be kept on password protected computer files.

The following guidelines are in place for staff to reduce the risk of personal data being compromised:

- Paper copies of data or personal information will only leave the locked office if deemed necessary. For example, all consent forms regarding users of BWC will be kept in a locked draw that is accessible to core staff as appropriate.
- Secure means should be used to destroy unwanted paper copies of data, sensitive data or other records, i.e shredding or burning. This also applies to handwritten notes that reference any child, vulnerable adult or staff member in any identifiable way. Notes written listing contact details must also be shredded.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in the printer tray or scanner.
- If information is being viewed or stored on a PC, staff must ensure that the window and documents are properly closed before leaving the computer unattended. All computers must be password protected and sensitive information should not be visible on guest accounts.
- If it is necessary to transport data away from the workplace, it must be downloaded onto a USB stick. USB sticks must be password protected at all times.
- Data shared across cloud-based storage systems, i.e droBWCox and one drive, should always be password protected.
- Data should not be transferred from this stick onto any home or public computer. Sensitive and personal data regarding CYP and vulnerable adults should not be stored on personal computers/devices

BWC will use reasonable efforts to safeguard all personal data and acknowledge that the use of internet and computers is not entirely secure. We therefore ensure that our employees who have access to any personal data are made aware of the seriousness of keeping such information protected. These guidelines are clearly communicated to all BWC staff and any person found to be

intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

7. Subject Access Requests (SARs)

BWC staff are entitled to see their own personnel files and know exactly what information is being stored about them and why. This is called a subject access request. BWC reserve the right to check the detail requested before agreeing or otherwise and will advise the individual in writing of the decision. Access may be denied or limited if the disclosure of such information involves a third party (e.g. a colleague), unless the third party concerned has given consent to the disclosure of that information.

BWC will respond to genuine SARs with:

- confirmation that their data is being processed;
- access to their personal data in an understandable format
- the appropriate privacy notice

All SARs should be made to a senior member of BWC External requests for information regarding an individual should not authorised without prior consent from the individual in question. Where appropriate, staff may agree to pass on the request to that individual to respond to if they choose to do so.

8. Guidelines for disclosing information to internal and external sources

8.1 Internal information sharing

BWC understands that trustees and staff may need to share personal information with others internally. This might include discussion of issues that arise during staff supervisions, discussion of situations to allow for opinions to be shared amongst the staff team and also for child protection matters. Care must be taken to ensure that the disclosure of such information is only done so on a 'need-to-know' basis and where it cannot be overheard. BWC will be transparent, when possible, and communicate the intention of how data will be shared with staff, parents/carers and CYP (subject to their age and understanding).

Personal information about a colleague should not be discussed with other staff or any one outside of the BWC organisation, unless authorised by the individual. Explicit consent from the individual is required prior to any sharing of address, phone number, health matters or personal circumstances. Confidential information discussed at Board meetings and staff meetings should not be disclosed outside of the organisation unless authorisation is given to do so. This does not apply to disclosures made under the Public Interest Disclosure Act ('whistle blowing). BWC staff members can find more guidance on the Whistle Blowing procedure in their Employee handbook.

8.2 External information sharing

Personal data regarding CYP will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Specific personal data held by BWC may be disclosed to the following parties without consent:

a) Health authorities
BWC may pass on information regarding the health of an individual in the event of a serious injury or accident occurring within the workplace. See Health and Safety Policy for more information.

b) Police and courts
If a situation arise where a criminal investigation is being carried out BWC may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

c) Social workers and support agencies
In order to protect and maintain the safety and welfare of all CYP who access our play sessions, and in cases of child abuse, it may be necessary for BWC to pass personal data on to social workers or support agencies. See Safeguarding and Child Protection Policy for more information on when a disclosure may be shared.

d) Funders
BWC stores and shares information when applying for funding, monitoring how funds are spent and when replying to funders. BWC only shares statistical information, such as the number of children/families/adults who have attended sessions including other required information in support of monitoring and evaluation including; genders, ethnicities. This ensures that full anonymity is kept. For publicity purposes BWC may also include quotes from our service users. The identity of the user must be anonymised unless the individual gives consent otherwise.

Any information needing to be shared outside of the organisation must be brought to the attention of senior members of the BWC staff team.

9. Staff obligations

The manager is recognised as the data controller and is responsible for notification to the Information Commissioner. He/she should be referred to with any questions relating to data protection or confidentiality. With this said, **all staff** are responsible for ensuring compliance with this policy. All staff must:

- Ensure that they have read and understood this policy as it relates to them
- Understand that all data discussed and shared must be up-to-date, accurate, fair and relevant, including personal information about themselves. Staff must notify the organisation of any changes in personal circumstances.
- Not keep records on other individuals which are unnecessary, incorrect or which contain opinions or speculation.

- Not share personal information about other members of staff or service users if discussed in a confidential manner, unless consent has been given.
- Keep all data secure. Paper evidence must be stored in a secure space, filed in date or alphabetical order. Computers and laptops must be password protected, stored in a locked room and must be properly shut down at the end of each day. Word documents and other files must not be left open on unattended computers.
- Never disclose or share any personal information relating to other staff, volunteers, trustees or services users outside of the organisation, unless explicit consent has been given by the individual.
- Personal data must be disposed safely, i.e shredded or burnt. This includes paper notes and records.
- When sending emails, staff must ensure that they do not copy in email addresses of those who have not given consent. To ensure this, multiple recipients should be blind copied (BCC) within the email.

10. Training

Individuals whose roles require regular access to personal data or who are responsible for implementing or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.

11. Notification of breaches

A breach of data protection can be defined as a security incident that has affected the confidentiality, integrity or availability of personal data. This includes situations were personal data is lost, destroyed, corrupted or unlawfully disclosed; the access or sharing of such data without appropriate consent; or if the data is made unavailable, for example, if it is accidentally lost or destroyed.

BWC has a duty to respond and when necessary, report personal data breaches to the relevant supervisory authority. Those informed, made aware or discovering a breach must report it to a member of BWC senior staff team. It is then up to the senior staff team to determine if this breach is likely to result in a risk to the rights and freedom of individuals, i.e. if the breach was to have a significant detrimental effect on an individual if left unaddressed. This can include a result in discrimination, damage to reputation, financial loss or loss of confidentiality.

If the senior staff team deem so, the breach must then be reported to the manager or if not available, the Chair of BWC Board of Trustees. Appropriate disciplinary action, in line with the 'Disciplinary procedure' found in BWC Employee handbook, will be taken and all breaches must be recorded. When necessary, serious breaches must be reported to the ICO.

Failure to observe this policy or misuse personal data is a disciplinary offence and may even constitute a criminal charge.

12. Date of policy and review

It should be signed by the most appropriate senior leadership figures (generally at trustee board level)

Policy agreed date: 2021

Glossary - *Definitions relating to GDPR and DPA*

Data	Information held on a computer or in a secured filing cabinet that identifies an individual. Data under the GDPR includes online identifiers such as IP addresses. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

Data controller	A person who determines the purposes for which and the manner in which any personal data is, or is to be, processed. Senior members of staff at BWC determine the purposes and means of processing personal data in a collective way. The Board of Trustees of BWC have overall authority over data control and processing. The controller is responsible for, and must be able to demonstrate, compliance with the Data Protection Principles (outlined in section 5).
Data subject	An individual who is the subject of personal data.
Subject Access Request (SARs)	A written or verbal request made by or on behalf of an individual for the information which he or she is entitled to ask for, under section 7 of the Data Protection Act 1998. The request does not have to be in any particular form.

Staff Confidentiality Statement.

Upon signing this statement, I acknowledge that I have read this policy and understand the reasons as to why The Bolton Woods Centre holds and shares information about me.

I understand my role and responsibility in relation to data protection and acknowledge that during my time at BWC I may learn facts about colleagues or individuals with whom BWC works. I recognise

that these facts may be of a personal and confidential nature and therefore agree to not disclose such information to any person not authorised by BWC. I agree to not hold personal or sensitive information without the permission of the individual or, in exceptional circumstances, the agreement of my line manager.

I agree to uphold a commitment to confidentiality both whilst I am working at The Bolton Woods Centre and in situations outside of work.

Signed: Date:

Name (Please print):