DATA PROTECTION RETENTION, SECURITY AND SAFE STORAGE POLICY

This policy will apply to CommUNITY Barnet and all its subsidiary organisations including Healthwatch Barnet, Healthwatch Brent, Healthwatch Newham, Volunteer Centre, and Wellbeing Hub; which will be collectively referred to in this document as CommUNITY Barnet.

Content

Policy Statement

CommUNITY Barnet is committed to the protection of the rights and freedoms of all individuals including staff, trustees, volunteer, service users, and community members in accordance with the provisions of the General Data Protection Regulation (GDPR). As such, CommUNITY Barnet will comply fully with the requirements of the regulation by:

1. Ensuring that all personal information is handled and dealt with in line with the regulation regardless of how it is collected, retained or used and whether it is held electronically, on paper or other formats.
2. Implementing procedures and procedures to ensure that all persons with access to personal data held by or on behalf of CommUNITY Barnet are fully trained and aware of the relevant policies and procedures.
3. Ensuring that all persons with such access to personal data will abide by their duties and responsibilities under the regulation in carrying out their CommUNITY Barnet roles.
4. Ensuring that accurate and proportionate records are kept to provide a good support framework for staff and volunteers, and to comply with employment, charity and company legal requirements.

In order to operate efficiently, CommUNITY Barnet collects and uses information about its staff (Past, current and potential), trustees, volunteer

and service users including donors and supporters and community members in order to deliver its services.

CommUNITY Barnet will ensure that all persons on whom information is held are notified and made aware of which data is held and how, why it is retained and for how long, and that they can request access to records held about them at any time.

In accordance with the principles of the Regulation, CommUNITY Barnet will ensure that the Information Commissioner's Office (ICO) is notified of its data processing activities.

The regulation relates to the processing of personal data and special categories of personal data (or sensitive data) which must be processed in accordance with the regulation's principles.

Definitions

Processing identifies a wide range of activities that include obtaining, recording, holding and storing personal data and carrying out any operations on such data including analysis, segmentation, adaptation, alteration, use for reaching the individuals in question, disclosure, transfer, erasure and destruction.

Personal and special categories of personal data refer to any information relating to an identified (directly or indirectly) or identifiable natural person ('data subject'). In particular, by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Service users: refer to all private individuals who do business with CommUNITY Barnet or any of its subsidiaries including donors and supporters and community members. Services received include but are not limited to information requests, websites' use, purchasing, making donations and or accessing goods and services.

Principles of the GDPR

The Regulation stipulates that anyone processing personal data must comply with its principles which are legally binding. The principles require that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
7. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).
8. Consent to the processing must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.
9. Processed in accordance to with Rights of the data subject.

Roles and Responsibilities

Data Management Structure:

1. Board of Trustees Data Lead – Has overall responsibility for data and data protection within CommUNITY Barnet, oversees data management, ensures the Senior Leadership Team (SLT) and the Board of Trustees are

aware of any changes or issues (such as data breaches) and act as the main point of contact with the ICO were required.

2. Data Champion Lead – responsible for:
a. Liaises with Data Champions to provide support, escalate issues and ensuring yearly data reviews are complete in accordance with the procedure,
b. Acts as link with the SLT/board by raise any changes, issues, breaches or concerns with the Trustees Data Lead,
c. Manages the centralised Information Asset Register, raise concerns and support the Board with new data requests,
d. Manages the process and supports the Board with incidents or data breaches
e. Liaises as required with the Policy Review Trigger Lead in managing policy and procedure reviews ensuring changes and updates are reflected in policies and fed through the organisation.

3. Data Champions – are responsible for:
a. Overseeing the team's data, ensuring accuracy confidentiality and security.
b. Assessing requests by their team for the collection of new data items and raise them with the Data Champion Lead for approval
c. Delivering yearly reviews of the data held by the team and delete/anonymise data as specified in the Record Retention Procedure
d. Managing the process in the event of a data breach in collaboration with the Data Champion Lead.

4. Policy Review Trigger Lead - responsible for:
a. Triggering Policy Review Procedure, liaising with staff responsible for specific policies to ensure they are reviewed, updated and adopted by the board with then set time scales,
b. Liaising with the Data Champion Lead as required to ensure policies and procedures remain consistent and relevant across the organisation while being compliant with GDPR.

Process

In line with the Regulation Principles CommUNITY Barnet will:
1. Appoint designated staff (Data Champions) with special responsibility for data protection to ensure data management is implemented in accordance to the regulation and ensure compliance at [your organisation]. Appointed staff will also be responsible for providing support and guidance to other members of staff and volunteers in their teams.
2. Ensure that staff and volunteer with access to personal data are aware of their roles and responsibilities and are adequately trained to handle that

data.
3. Ensure personal data is collected in a specific, explicit and unambiguous manner and for a legitimate stated purpose through adequate procedures on and off line; ensuring that we have a clear and unambiguous indication of the data subjects' agreement for their data to be processed.
4. Ensure that data subjects can exercise their full rights as stated in the Regulation. These include the right to be informed how their data will be used, the right to access one's personal information, the right to rectify, erase, object and restrict processing in certain circumstances and their right to data portability.
5. Ensure that personal data is processed lawfully, fairly and in a transparent manner through appropriate management and systems.
6. Collect and process appropriate data only to the extent that it is needed to fulfil operational needs or to comply with legal requirements, that it is kept secure, it is accurate and held for no longer than is necessary.

The Responsibilities of Employees

All employees at CommUNITY Barnet are required to:
1. Attend relevant trainings and workshops aimed at improving knowledge and understanding of the regulation and how to implement it in their day to day activities.
2. Ensure they understand the provisions of the Regulation and understand their responsibilities in relation to personal information they may process while undertaking their duties.
3. Seek guidance and support from line managers and Data Champions if they are unclear as to the application of the Regulation or are uncertain as to how to handle a given situation.
4. Ensure that all data collection processing storing and use is done in accordance with the regulation and this policy. More specifically they will ensure that:
a. All files and document containing personal data held on paper, electronically or otherwise are kept secure at all times and protected against unauthorised, unlawful loss or disclosure.
b. All electronic files, documents and emails and computer systems where personal data can be accessed are password protected at all times and in such a manner that the password cannot be easily compromised.
c. They safely and securely logout of any systems, networks, apps, computers, laptops and other mobile devices if they are to leave such systems unattended for long periods of time and at the end of each working day, to reduce the risk of breach or data hacking.
d. All drawers and cabinets containing personal data are securely locked at all times.
e. Personal information is not disclosed verbally, in writing, via email, web or any other means accidentally or otherwise to an unauthorised third party.

f. All data is collected via approved processes and procedures which have been signed off and approved by the board.
g. Data Champions and line managers are consulted and made aware of any new personal data the member of staff or team intends to collect for any given purpose to ensure these are covered by the CommUNITY Barnet data protection policies and procedures.
5. In relation to their own personal data, employees will ensure that any information provided in connection with their employment is accurate, up to date and that they will inform CommUNITY Barnet of any changes to their circumstances.
CommUNITY Barnet will be ultimately responsible for all data collected and processed by the organisation. If an employee discloses personal data in breach of the principles set out in the Regulation, they may be committing a criminal offence and may be subject to disciplinary action.

Data in Transit
Should the need to take files containing personal data outside the office arise, members of staff will be personally responsible for taking reasonable and appropriate precautions to ensure all personal, sensitive and confidential data taken outside of the office is secure and kept safe at all times. This includes data in all formats including but not limited to paper and electronic storage such as laptops, tablets, pads and removable storage (e.g. USB memory sticks and external drives), mobile phones or any form of networking equipment).
Any data loss must be reported immediately to the employee's line manager who will assess the situation and impact and agree the necessary action.

Contractors
All contractors with access to personal data supplied by CommUNITY Barnet will be required to confirm in writing that they will abide by the requirements of the regulation with regard to all CommUNITY Barnet information provided and/or accessed via but not limited to paper or electronically. Contractors will be required to ensure that they and their staff who have access to personal data held or processed for, or on behalf of, CommUNITY Barnet are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the regulation. (See Information and Data Sharing Policy).

Subject Access Request
Individuals whose data is held by CommUNITY Barnet have the right to request access to their personal data, through a Subject Access Request. Service users, donors, supporters and members of the public and all persons excluding employees whose personal data is held by [your organisation], or who believe that CommUNITY Barnet may hold their data,

may make a Subject Access Request in writing, to the Helen Harte, Head of Business Development, to receive a copy of the information held on them. CommUNITY Barnet will respond to all requests for personal information within 30 days of the request.

Employees may request details of their personal data held by CommUNITY Barnet by notifying their line manager. If an employee believes that any information held on them is incorrect or incomplete they should write to their line manager as soon as possible setting out the information which they believe needs correction.

Confidential References
1. Copies of confidential references about employees written by CommUNITY Barnet will not be provided in response to Subject Access Requests.
2. Confidential references about employees received by CommUNITY Barnet are not exempted. CommUNITY Barnet will make reasonable attempts to gain consent from referees prior to release. If consent cannot or will not be given CommUNITY Barnet will permit release if satisfied that to do so would not prejudice the interests of the referee.

Notifying the ICO (Information Commissioner's Office)
CommUNITY Barnet will notify the ICO as appropriate of its processing of personal data and ensure the updating of the information if there has been a serious breach of Data Protection.

Record Keeping
All records of services users, staff, trustees and volunteers are confidential and will be held securely and in accordance with CommUNITY Barnet guidance.
All records will be stored in lockable filing cabinets and/or in secure password protected and regularly backed up online files and will be kept up to date by the data owner and/or administrator.

Access for this normal maintenance of the file and for supervision purposes is not recorded. A note of all other access for specific purposes will recorded on the record log, including access by the users or CommUNITY Barnet for quality assurance purposes.

Right to work documentation
The Home Office's guidance "An employer's guide to acceptable right to work documents" provides the following 3 steps:
1. Obtain original versions of one or more acceptable documents
2. Check the document's validity in the presence of the holder
3. Make and retain a clear unaltered copy of all documents checked

(hardcopy or scanned unaltered copy in jpeg or pdf format), and record the date on which the check was conducted and by whom. This may be by either making a dated declaration on the document copy or by holding a separate manual or digital secure record, indicating the date on which the check was conducted, the documents copied and by whom. The date of check may be written as follows: 'the date on which this right to work check was made: [insert date]'.
The full "An employer's guide to acceptable right to work documents" guidance document can be found here: (https://www.gov.uk/government/publications/acceptable-right-to-work-docu...).

User Records
Users will be informed at the initial contact (and at any subsequent contact where additional personal data may be collected) that a record will maintained about them for the purpose of providing the required service, how long the record will be kept for, they will be informed of their rights to access their data and their consent to use the data for the defined purpose will be clearly and unambiguously sought. This will be communicated verbally or electronically depending on the nature of the contact and clear and accessible guidance and policies will be available to user on all websites. Once service delivery has ceased data will be retained and destroyed/anonymised in accordance with the CommUNITY Barnet Record Retention Procedure. Where it is a requirement of, a funder or Local Authority to retain records for a longer period, the time frame may change. This will be clearly documented, and users will be informed accordingly.

Volunteer Records
Selection and appointment information including supervision meeting notes will be retained. Supervision notes will be signed by the supervisor and the volunteer and stored in the appropriate section of the volunteer file.
When a volunteer leaves the scheme, the volunteer file will be retained and destroyed in accordance with the CommUNITY Barnet Record Retention Procedure and destroyed at the appropriate date.

Volunteers will be informed that a record is maintained about them, that they have the right to request access to it, and that the file may be sampled by CommUNITY Barnet for the purposes of Quality Assurance.

Staff and Trustee Records
Selection and appointment information, absence, sickness and accident records will be retained in line with the CommUNITY Barnet Record Retention Procedure, and destroyed at the appropriate date.
A written record of each supervision and appraisal meeting with the member of staff is made and signed by the line manager and the member

of staff. The member of staff retains one copy and a second is stored in the staff's personnel file.

When the member of staff or trustee leaves, the personnel file will be retained and destroyed in accordance with the CommUNITY Barnet Record Retention Procedure, and destroyed at the appropriate date.

Compliance

CommUNITY Barnet will:

- Comply with the requirements of company law by retaining required records
- Comply with the Statement of Recommended Practice (SORP) in relation to its financial record Retention and reporting
- Stores insurance policies and employer's liability insurance certificates
- Stores documents relating to the ownership or leasehold of premises

The above records will be retained securely and in accordance with the CommUNITY Barnet Record Retention Procedure specified in this policy and will be destroyed at the appropriate date.

Disclosure Information (DBS Certificates)

General Principles

CommUNITY Barnet undertakes DBS checks to help assess the suitability of applicants for positions of trust. As such CommUNITY Barnet fully complies with legislative procedures and recommended codes of practice regarding the correct handling, use, storage, retention and disposal of Disclosure Information. CommUNITY Barnet also complies fully with its obligations under the GDPR and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Disclosure Information.

Usage

CommUNITY Barnet will only use disclosure information for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Any matter revealed in a disclosure will be discussed with the person seeking the position before withdrawing a conditional offer of employment or deciding that a prospective volunteer or trustees is not suitable for role applied for. Having a criminal record will not necessarily bar an applicant from working at CommUNITY Barnet. This will depend on the nature of the position and the circumstances of the offences disclosed. (See CommUNITY Barnet's policy on the recruitment of ex-offenders.)

Storage, Access & Handling

CommUNITY Barnet will ensure that original disclosure certificates or copies of such certificate are not kept longer than the 6 months period specified within the Record Retention Procedure. Where a copy of an

original document is retained for the allowed 6 months period it will be stored separately and securely, in a lockable/password protected and non-portable storage with access strictly controlled and limited to those with authorisation to access it as part of their duties.
Notwithstanding the above, CommUNITY Barnet will retain the following on the volunteer file:
- the name of the individual
- a record of the date of issue of their Disclosure
- the type of Disclosure requested
- the position/purpose for which the Disclosure was requested
- the unique reference number of the Disclosure
- details of disclosure information
- the details of the recruitment decision taken.

Subjects of a DBS check will be informed of the relevant Code of Practice and a copy will be available on request.
Legislation requires that Disclosure Information should only be shared with those who are authorised to receive it in the course of their duties. CommUNITY Barnet recognises that it is a criminal offence to share this information with anyone who is not entitled to receiving it. A record will be maintained of all those to whom disclosures or Disclosure Information has been revealed.
Retention
Please refer to the Record Retention Procedure associated with this policy.
Disposal
Once the retention period has elapsed, as detailed in the Record Retention Procedure, disclosure information will be immediately and suitably destroyed by secure means, i.e. by shredding, pulping or securely deleting electronically held data. While awaiting destruction, Disclosure Information will continue to be kept safely and securely. Paper versions will not be stored in unsecure storage such as recycle bin or confidential waste shredding sack.
Board of Trustees Data Lead
Michael Lassman
CommUNITY Barnet
Barnet House
First Floor, 1255 High Rd
London N20 0EJ

Policy Authorisation and Adoption

Adoption date: 01/08/2018

Name: Julie Pal

Review Date: 01/08/2019