DATA PROTECTION AND DATA STORAGE POLICY

1. Purpose and Scope

1.1 This Data Protection and Data Storage Policy (the “Policy”) applies to all personal data collected and dealt with by Centre 404, whether on paper, in a computer or recorded on other material.

1.2 The purpose of the Policy is to enable Centre 404 to comply with privacy and data protection laws including the Data Protection Act 1998 (the “DPA”), to follow good practice guidance, and to ensure that Centre 404 takes adequate measures to protect such personal data which has been gathered, processed and stored at any Centre 404 office.

1.3 Following the Policy, Centre 404 aims to:

- comply with both the law and good business practice;
- respect individuals’ rights;
- be open and transparent with individuals whose personal data is held by Centre 404; and
- provide training and support for its staff and volunteers who handle personal data, so that they can act confidently and consistently.

1.4 Any material breach of this policy will be dealt with under Centre 404’s disciplinary procedure as outlined in the staff handbook.

2. Review

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the DPA.

3. Data Protection Principles

3.1 Centre 404 regards the lawful and correct treatment of personal data as very important to successful working and to maintaining the confidence of those with whom Centre 404 works.

3.2 Centre 404 will adhere to the principles of data protection (“the Principles”), as detailed in the DPA. Specifically, the Principles require that personal data:

- shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
shall be obtained only for such purpose(s) as specified under the DPA, and used only in ways that are compatible with such purpose(s);
shall be adequate, relevant and not excessive in relation to those purpose(s);
shall be accurate and, where necessary, kept up to date;
shall not be kept for longer than is necessary;
shall be processed in accordance with the rights of data subjects under the DPA;
shall be kept secure by Centre 404, who shall take appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information;
shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to processing their personal data.

4. Responsibilities

4.1 In order to protect Centre 404 from the consequences of a breach of its responsibilities, all staff, consultants and volunteers are required to read and understand their responsibilities as outlined within the Policy. If staff, consultants and volunteers are uncertain of their responsibilities in relation to data protection, they are required to seek guidance from the Resources Manager at Centre 404.

4.2 The Board of Trustees and the Chief Executive each recognises their overall responsibility for ensuring that Centre 404 complies with its legal obligations in relation to data protection, but it is the responsibility of all staff, consultants and volunteers who deal with personal data to ensure that Centre 404 complies with this Policy.

4.3 The Personnel Committee will review any amendments and updates in relation to data protection, and present any recommendations to the Board of Trustees.

4.4 The Resources Manager and Heads of Service are responsible for advising staff on data protection issues and procedures relevant to their role and for ensuring that relevant training and inductions take place.

4.5 Volunteers are required to comply with procedures relating to the handling of personal data and confidentiality as described in their volunteer agreement and handbook.

4.6 Staff who are required to produce monitoring and evaluation reports or documentation (for example, statistics or reports demonstrating staff
absence or statistics and reports that relate to our work with service users and volunteers) must only display information anonymously.

5. Safe Management of Personal Data

Centre 404 will, through appropriate management and the application of its systems and guidelines:

- fully observe conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, to the extent such information is needed to fulfil its operational needs or to comply with any legal requirements;
- ensure that Heads of Service are responsible for monitoring the quality of the information used and that personal data relating to staff, volunteers, consultants and service users is accurate and up to date;
- ensure that the rights of individuals about whom information is held, can be fully exercised under the DPA. These include:
  
  - the right to be informed that processing is being undertaken;
  - the right of access to one’s data;
  - the right to prevent processing in certain circumstances; and
  - the right to correct, rectify, or delete information which is regarded as wrong information;

- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards;
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information; and
- set out clear procedures for responding to requests for information.

6. Security and Data Storage

6.1 Departmental procedures for collecting, handling, processing and storing personal data about staff, volunteers, service users and others having a commercial relationship with Centre 404 are in place and will be covered in induction and staff training.

6.2 All recruitment information and documentation is stored confidentially by the Central Team. Only essential staff and volunteers involved in the
administration and selection and recruitment process should have access to application forms that have been submitted. Care should be taken to ensure that diversity monitoring, Criminal Records Bureau disclosure information and other sensitive information relating to individuals is handled appropriately in line with recruitment guidelines.

6.3 Written consent should be obtained from service users and volunteers when personal data is collected and individuals should be given the opportunity to say if they do not wish certain information to be recorded or passed on to a third party. Staff will also be required to explain why they are gathering the data and for what purpose(s) it will be used.

6.4 Any personal data that is collected about staff, volunteers, consultants, service users or others having a commercial relationship with Centre 404 will be stored securely and confidentially. Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers. Any staff planning to take any documents or electronic storage devices (including laptops and USB sticks) that contain personal data off the premises must obtain prior permission from their relevant head of service. The storage of any personal data collected by Centre 404 at any personal address or location that is not an authorised Centre 404 office or workplace is strictly prohibited.

6.5 Electronic information that contains personal data must be stored in the relevant folder on the shared drive (not on individual hard drives), be clearly labelled and identifiable and password protected. Staff accessing electronic data files from home or other locations must to comply with this policy at all times to ensure any personal data remains protected.

6.6 Heads of Service are responsible for ensuring that staff follow procedures relating to using and sharing passwords for data that is stored electronically (including email records) and for permitting access to paper filing systems. Permission to access electronic folders stored on the server should be authorised by Heads of Service.

6.7 Heads of Service are required to provide a list of all types of personal data collected, how and where it is stored and who has access. This list is to be held centrally with the Resources Manager and shall be updated annually as required.

6.8 Staff must report all incidents where any form of personal data and/or devices containing personal data have been lost, misplaced or stolen as a result of transporting personal data records outside of any Centre 404 office or project location, to the relevant Head of Service and Resources Manager.
so that any appropriate remedial action or reporting processes can be followed.

7. **Misuse of Access to Personal Data**

7.1 Staff, volunteers and consultants that have been permitted access to personal data records as part of their work with Centre 404 are required to sign a confidentiality agreement to show that they have read, understood and accept their responsibilities in relation to data protection.

7.2 Where any individual at Centre 404 believes that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be sanctioned with the authorisation of the relevant Head of Service or Resources Manager. All such disclosures will be documented and reported to the Chief Executive.

7.3 Significant breaches of this policy will be dealt with under Centre 404’s disciplinary procedure; serious breaches may be considered gross misconduct, for which a sanction of dismissal may be imposed.

8. **Access to files (upon leaving employment/volunteering)**

Heads of Service and line managers are responsible for ensuring the following procedures are followed when a member of staff, volunteer or consultant resigns from their role at Centre 404:

- All keys to property are returned to the central team or housing project manager and recorded as such on the relevant key register. Keys to filing cabinets and cupboards should be returned to the relevant line manager;
- The relevant individual’s accounts and passwords for access to electronic or shared drives and internet-based applications are changed or deleted;
- If email accounts are no longer required the account should be deleted;
- Staff that have Centre 404 email accounts should be informed before they leave that new incoming employees may be given access to their email account in order to ensure continuity of service delivery; and
- All devices for storing and transporting electronic information (datakeys, external hard drives etc) are returned to Centre 404 or cleared of personal data prior to leaving.

9. **Document Retention**

9.1 Personal data will be stored for only as long as it is needed or required under the DPA and will be disposed of appropriately. No personal data should be retained for more than five years after it is no longer needed.
9.2 Paper records and documents that hold personal data should be stored in a secure and lockable cabinet, and where possible a fire proof cabinet, to protect them from fire damage, and clearly labelled to ensure that any personal data contained within them remains confidential and secure.

9.3 Archive storage, if applicable, must be clearly labelled and marked private and confidential and where possible stored in a secure location with limited staff access. A record of the location, box number and date of disposal of all archive storage should be copied to the Resources Manager for information.

9.4 Electronic archiving is overseen by the Resources Manager in consultation and agreement with the designated IT Support contractor (Thames Computer Services), according to the procedure as set out in the IT folder in Central Office.

9.5 Heads of Service are responsible for managing the safe and appropriate disposal of records in accordance with the recommended guidelines. The Resources Manager is responsible for managing the safe disposal of any archived material that is stored within the central archives.

9.6 Each service area will use a data schedule that includes details of the type of data and documentation collected, how it will be used and stored, who has access to it, how consent is gained from the data subject and how long it should be kept for. Data schedules will be available to all staff for information in their service area handbook and held and updated by Heads of Service.

10. Informed Consent

10.1 Informed consent is when a data subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data, and who then gives their consent.

10.2 Centre 404 shall ensure that informed consent has been obtained from individuals prior to using any personal data for use on Centre 404’s website, social media outlets, leaflets, promotional material and mailing lists.

10.3 Informed consent should always be obtained prior to using any personal data including photographs, names, age and information relating to a disability, personal circumstances or services that individuals have received at or from Centre 404 prior to publication and circulation.

10.4 Centre 404 will ensure that personal data is collected within the boundaries defined in this Policy, and shall ensure that the data subject:
clearly understands why the personal data is needed;
- understands what it will be used for and what the consequences are should the data subject decide not to give consent to processing;
- as far as reasonably possible, grants explicit consent (either verbally or in writing) for data to be processed;
- is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress; and
- has received sufficient information on why their data is needed and how it will be used.

11. Requests for the Disclosure of Personal Data

11.1 Individuals have a right to know what information is being held about them.

11.2 In response to a valid data subject access request (including the fee, if required), Centre 404 must provide a permanent, intelligible copy of all the personal data about that data subject held at the time the application was made. Centre 404 may negotiate with the data subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld.

11.3 Data subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Resources Manager or Head of Service without delay.

11.4 In some cases Centre 404 may have a legal obligation to disclose personal data. In such cases Centre 404 will ensure that it only discloses information that has been specifically requested. Where it is permitted and practicable Centre 404 will endeavour to inform individuals as to what information is being requested, by whom and why.

11.5 All data subject access requests and disclosures must be reported to the Resources Manager, and records kept of any documentation and correspondence issued and returned.