GRASSROOTS Confidentiality and Data Protection Policy

1. Introduction

(A) GRASSROOTS recognises that, in the context of our work, we come into contact with people from a variety of diverse backgrounds and deal with potentially sensitive individual and community issues. Consequently it is essential for maintaining trust and developing relationships that information is treated appropriately. This policy sets how we will record, use and store information, how, with whom and under what conditions it will be shared and how individuals can access the information.

(B) For employees it is a condition of employment that a breach of this confidentiality policy will be dealt with as a serious matter and serious breaches may result in dismissal. The responsibility to adhere to this policy persists even after a person has ceased to be an employee/volunteer with GRASSROOTS.

(C) The General Data Protection Regulations (GDPR) and Data Protection Act (2018) regulate the way information about living identifiable people is collected, used and stored.

(D) In compliance with these, GRASSROOTS will ensure anyone with whom it works (e.g. employees and applicants, volunteers and personnel in partner agencies) are aware of the reasons for collecting and using any personal data, and will only collect and store data with their explicit permission.

(E) We hold the following data:

1. *Organisational Information* –
   This is publicly available information about organisations and some confidential information (such as office/employee contact numbers which are for partner agencies and not for public use)

2. *Personal Information – Public*
   This is information about individuals such as names, addresses, phone numbers and e-mail addresses for the purposes of advertising our work and events etc

3. *Personal Information – Personnel*
   This is about employees (employed and voluntary) as necessary for maintaining relevant records (including DBS checks as our community work involves employees engaging with children, young people and vulnerable adults)

(F) Any trustee, employee or volunteer has the right to see what information is held on file about them by sending a request to do so to the Director.

2. Data Protection Principles

(A) GRASSROOTS shall actively adopt The Six Privacy Principles of GDPR in both policy and practice, as outlined in Appendix A.

(B) GRASSROOTS will only collect information for "specified, explicit and legitimate purposes" [GDPR, Article 5, clause 1(b)].

(C) GRASSROOTS will not hold information about individuals without their knowledge and consent, and they shall be informed of how the information is processed and stored.

(D) GRASSROOTS will only hold information for specific purposes and inform individuals what those purposes are. It will also inform them if those purposes change.

(E) Information obtained about people through unofficial channels (for example, by gossip or hear-say) should not enter GRASSROOTS' information system except where non-disclosure may lead to either a legal risk or a risk to anyone's health or safety.

(F) Information held will be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [GDPR, Article 5, Clause 1(c)].

(G) Information will be "kept in a form which permits identification of data subjects for no longer than necessary" [GDPR, Article 5, Clause 1(e)].

(H) The information that GRASSROOTS holds will be "accurate and where necessary kept up to date" [GDPT, Article 5, Clause 1(d)].

(I) Individuals will be entitled to have access to information held about them by GRASSROOTS, unless the information compromises the confidentiality of a third party.

(J) Individuals will be entitled to request the deletion of any and all records that GRASSROOTS may hold about them.

(K) Information about individuals will not be disclosed to other organisations or individuals except in circumstances where there is explicit or implied consent, where the information is publicly available elsewhere or, exceptionally, where it is deemed necessary without prior consent. Such circumstances could include disclosure to the police or law enforcement agency, Social Services where the well-being of the individual or any other person may be in question, a health service professional (e.g. paramedic, doctor or nurse) or any organisation covered by statutory order where failure to disclose would undermine the legal obligations of GRASSROOTS.

(L) GRASSROOTS has procedures for ensuring the security of all personal data, which will be handed "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [GDPR, Article 5, Clause 1(f)].

a. Paper records containing confidential personal data are stored and disposed of in a secure way. Employees and personnel records (including DBS disclosure information) are held in a locked filing cabinet with regulated access. Disposal will be by shredding, pulping or burning and we will not allow any personal data to be kept in an insecure receptacle while awaiting disposal.

b. Electronic records shall be held on password protected laptops which are to be kept safely in a locked filing cabinet, in person with the relevant employee or volunteer, or securely in the home or car (when being transported) of the relevant employee or volunteer. Where possible, external hard drives shall be password protected and/or encrypted.

(M) DBS disclosure information is only passed to those authorised to receive it in the course of their duties. In accordance with section 124 of the Police Act (1997), it is a criminal offence to pass this information to anyone who is not entitled to receive it. The disclosure will be destroyed within 6 months or once the applicant or employee has been deemed suitable for their role. A record will be kept of the disclosure date of issue and number - should funders require further proof the employee will need to produce their original of the disclosure.

(N) There may be situations where GRASSROOTS works in partnership with other organisations on projects which require data sharing. GRASSROOTS will clarify which organisation is to be the Data Controller and will ensure that the Data Controller deals correctly with any data which GRASSROOTS has collected.

(O) All new employees will be given training on the data protection policy and procedures.

(P) GRASSROOTS will carry out regular reviews of its data protection policy and procedures, especially if requirements change.

3. Protection of this policy

(A) Any employee or volunteer and any person with whom GRASSROOTS works has the right to complain if they feel their confidentiality has been breached in any way.

(B) Any member of the employee/volunteer team, who becomes aware of another employee/volunteer misusing confidential information or in breach of this policy, must report it immediately to the GRASSROOTS Director or to a Trustee.

Appendix A - The Six Privacy Principles of GDPR