Confidentiality Policy

Dunbar Area Christian Youth Project (DACYP) is committed to maintaining high standards of confidentiality. This policy document gives guidelines on how this should be achieved and explains the circumstances where disclosure of confidential information may be necessary.

SCOPE

This policy relates to everyone working for, or volunteering with DACYP and are henceforth referred to as 'personnel'. Any information that identifies an individual directly or indirectly is personal data as defined by data protection law currently General Data Protection Regulations (GDPR) and must be treated in accordance with that Law.

POLICY

Personnel should not normally divulge to any third party, or otherwise make use of, information of a confidential nature which comes to your knowledge, your possession or remit during or after your employment or voluntary work with DACYP.

CONDUCT

1. In most cases, information will not be explicitly stated as 'confidential', and personnel will need to exercise common sense and discretion in identifying whether information is expected to be confidential.

2. Personnel should always respect the confidentiality of any professional relationship but should never give an absolute guarantee that conversations, particularly around safeguarding, illegal or immoral matter, can remain confidential.

3. Where issues are raised that need to be brought to the attention of others (e.g. Youth Worker, Chair of Management group) this should be made clear to the individual.

DUTY TO DISCLOSE INFORMATION

1. There may be a legal duty to disclose information particularly if a person has done, or intends to do, serious harm to themselves or others, or if they pose a significant risk to others. This would include matters relating to Safeguarding issues.

2. Where possible and appropriate, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

ACCESS TO AND STORING OF INFORMATION

1. Confidential information must only be accessed by staff/ personnel who need it to fulfil their role or on a genuine need-to-know basis.

2. All data should be stored securely. If in paper form it should be in a locked cabinet. If in electronic form it should **not** be stored on a shared/public computer. It should be password protected.

3. All data should be reviewed regularly (at least once per year) to ensure it is accurate and that we are not holding unnecessary data.

4. Data no longer required should be deleted/shredded.

5. Any data we hold should not be shared with third parties.

6. Any emails sent out to circulation lists should use BCC. No one should be able to 'Reply All' to our mailings.

7. All general emailing should include the option to Unsubscribe with clear instructions as to how to do so.
   Example wording: *If you no longer wish to receive news updates from DACYP please reply to this email and mark 'Unsubscribe'. Thank you.*

BREACH OF CONFIDENTIALITY

1. Any loss or potential breach of confidentiality must be reported to DACYP Youth Worker or the Chair of the DACYP Management Committee, or one of the Trustees.

2. Personnel breaching confidentiality or accessing unauthorised files or information they have no authority to access will face disciplinary action, including dismissal.

3. Where personal data is concerned, unauthorised access may also be a criminal offence.