D&G HandyVan (SCIO)
Privacy and Confidentiality Policy

1 Introduction

1.1 D&G HandyVan (SCIO) acknowledges that its employees, volunteers and Board members may gain information about individuals during the course of their work.

1.2 D&G HandyVan (SCIO) recognises that confidential material should be kept confidential and will comply with the Data Protection Act 1998.

2 Aims of the Policy

2.1 To ensure that D&G HandyVan (SCIO) employees, volunteers and Board members recognise what information is confidential and what is not.

2.2 To ensure that confidential material remains confidential within the D&G HandyVan (SCIO).

2.3 To ensure that confidential material is stored correctly and in accordance with the Data Protection Act 1998.

3 Application of the Policy

3.1 All employees, volunteers and Board members shall receive a copy of this policy and subsequent updates.

3.2 Employees and volunteers should use common sense when receiving any information. If they are unsure whether it is confidential or not they should consult with their line manager.

3.3 All information, whether confidential or not, can be shared with the employee's line manager.

3.4 Employees and volunteers should not exchange information they have gained either professionally or privately with anyone else in a social setting.

3.5 On occasions where employees/volunteers need to discuss an individual to solve a difficult problem, this can be done provided the individual gives permission. Alternatively, a discussion may take place where the individual names are changed.

3.6 Where there is a legal duty to disclose information, the person to whom confidentiality is owed will be informed of the disclosure.

3.7 Anyone finding material they suspect may be confidential, which is either unlabelled or badly labelled, should report this to their line manager immediately.

4 Confidential material

4.1 Examples of material that should be kept confidential include:

- Personal information about employees, volunteers, Board members or other individuals, for example:
- Full names, personal addresses, telephone numbers
- Contact details which the individual has requested to be kept confidential
- Dates of birth
- Bank details
- National Insurance Numbers
- Disclosures
- Details about disciplinary action
- Information about ethnicity, sexual orientation and preference, disabilities, etc gathered for purposes of monitoring equal opportunities.

5 Access to information stored

5.1 Information is kept confidential within D&G HandyVan (SCIO) and can be passed to employees and the Board where relevant.

5.2 Information that is confidential should have access restricted to the employee who obtained it and their direct superiors. If written down it should be clearly marked 'Confidential – for Manager/Board access only' and should be stored suitably. This includes computerised files.

5.3 Employees must not withhold information from their line manager except in exceptional circumstances.

5.4 Any individual about whom D&G HandyVan (SCIO) holds information is entitled to see any information kept on them. To request a viewing they should write to the Chair giving 14 days' notice. In a case where the information is marked confidential it can only be viewed by individuals named on the file.

5.5 Employees may view their personnel records, and are required to give 14 days' notice to view them.

5.6 When photocopying or viewing confidential documents on a computer, employees should ensure that no one passing views their content.

6 Storage of Material

6.1 Non-confidential material should be stored in a filing cabinet with access to all employees and the Board.

6.2 Information about volunteers and/or individuals should be kept in a filing cabinet with access only given to the employee responsible for the records and their line manager. It should be kept locked at all times.

6.3 Employees' personnel files should be kept by the manager in a locked filing cabinet with access given to the Chair or member of the Board should they require it.

6.4 Files and filing cabinet drawers containing confidential material should be clearly marked as confidential.

6.5 The Chair may authorise other employees to view any files in emergency situations.

6.6 Any confidential material that needs to be destroyed as it has expired must be done securely by either shredding or burning. The person responsible for this must ensure that this is done correctly and may face disciplinary action if the material they destroyed is found.

6.7 Confidential material stored on computers and other electronic equipment must be treated with the same care as if it was written down.

6.8 It should be stored in a file marked private and confidential with a "read me" file giving details on who has the right of access, in the folder with the folder of confidential material. The file itself should be password protected with the password only given to the people on the access list.

6.9 When deleting electronic confidential material, care should be taken to ensure that all copies of it are removed, including the recycle bin.

7 Duty to Disclose information

7.1 There is a legal duty to disclose certain information. This includes:

- Information relating to child abuse should be reported to the Police.
- Any activities considered a criminal offence should be reported to the police, for example drug trafficking and money laundering.
- If an employee suspects a colleague of taking part in an illegal act, or that they may harm themselves; this should be reported to the Chair who should inform the police.
- Any disclosures of this type must be reported to the Chair and the soonest possible time.
- In all cases of disclosure the individual concerned must be informed of the disclosure.

8 The Data Protection Act 1998

8.1 Information kept about individuals falls under the Data Protection Act 1998 and must comply with data protection principles. Under the Data Protection Act 1998 personal information must be:

- Obtained and processed fairly and lawfully
- Held only for specific purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with the Act
- Kept securely and protected
- Not transferred out of Europe

Any breaches of the Data Protection Act will lead to prosecution.

9 Breaches of Confidentiality

9.1 If any employee feels dissatisfied by the conduct or action of their colleagues or the D&G HandyVan (SCIO) they should raise this with their line manager using the grievance policy.

9.2 Employees should not discuss work-related dissatisfaction outside the D&G HandyVan (SCIO).

9.3 Colleagues deliberately accessing confidential files and information that they are not authorised to will face disciplinary action.

9.4 Former employees breaching confidentiality will face legal action.

9.5 For further clarification refer to D&G HandyVan (SCIO) Whistleblowing Policy

10 Updating and amending

10.1 This policy shall be reviewed annually.