The DASH Club
Possilpoint Community Centre
130 Denmark Street
Glasgow, G22 5LQ

Mary Tel: 0141 336 8852
Sean Tel: 0141 336 8546
office@dashclubglasgow.org.uk
www.dashclubglasgow.org.uk

DATA SECURITY POLICY

Registered Charity No: SC031921 Company No: 38757

Data Security Policy
(May 2018)

1. About This Policy

1.1 We have put in place procedures and technologies to maintain the security of all our personal data, including the data of our clients or other personal data that is collected or held through DASH activities. Data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

1.2 This policy does not form part of any employee's contract of employment and may be amended at any time.

1.3 If you consider that this policy has not been followed you should raise the matter with the DASH Club Manager.

1.4 Any breach of this policy will be taken seriously and may result in disciplinary action, up to and including summary dismissal.

1. Data Security

1.1 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is provided and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

1.2 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required in accordance with the Data Protection Policy.

Equipment. Employees, contractors, volunteers should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.