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 PROTECTION POLICY

Registered Charity No: SC031921 Company No: 38757

The DASH Club Data Protection Policy

(May 2018)

1. About This Policy

1.1 The DASH Club ("DASH") is committed to being transparent about how we collect and use the personal data of our young people and their families and DASH staff, and to meeting our data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 This policy applies to all personal data we collect from our young people, our staff (past and present), potential staff, volunteers, contractors and our Board Members.

1.3 DASH has appointed a Data Protection Officer, please contact the DASH office for their name and contact details. They have responsibility for data protection compliance within DASH. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

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

1.5 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with the Data Protection Officer.

2. Definitions

2.1 **"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

2.2 **"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

2.3 **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3. Data Protection Principles

3.1 DASH holds personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

3.2 We will tell you the reasons for processing your personal data, how we use such data and the legal basis for processing in its privacy notices. We will not process personal data of individuals for other reasons.

3.3 Where DASH processes special categories of personal data or criminal records data to perform obligations or to exercise rights in law, this is done in accordance with this policy and with relevent legislation.

3.4 We will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

3.5 Personal data gathered during the relationship you have with DASH is usually held in a special file (in hard copy or electronic format, or both), and on DASH systems. The periods for which the Organisation holds personal data are generally for the period that the relationship is on-going or could reasonably be expected to be on-going as it hasn't been terminated, and following a specified termination to the relationship, for a period not more than 6 months. Unless there is a lawful reason that DASH should keep such information.

3.6 We keep a record of our processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. Individual Rights

4.1 Individuals have a number of rights in relation to their personal data.

4.2 You have the right to ask us for information about the personal information we hold about you. This is called a subject access request. If an individual makes a subject access request, DASH will tell him/her:

- whether or not his/her data is held and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.
- Where the request is from a Parent or Guardian on behalf of a child we have the obligation to consider whether the child is mature enough to understand their rights in relation to their personal information, and respond accordingly. We will act in the best interests of the child.

4.3 We will also provide you with a copy of the personal data held if you would like this. This may be in electronic form or a hard copy, depending on the type of information requested and held.

4.4 If you want additional copies, we will charge a fee, which will be based on the administrative cost to DASH of providing the additional copies.

4.5 To make a subject access request, you should send the request to the DASH office. In some cases, DASH may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify his/her identity and the documents we require.

4.6 The Organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Organisation processes large amounts of the individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell him/her if this is the case.

4.7 If a subject access request is manifestly unfounded or excessive, DASH is not obliged to comply with it, and will tell you if this is the case. Alternatively, DASH can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request which DASH has already responded to.

5. Other Rights

5.1 You have a number of other rights in relation to your personal data. You can require the Organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of which it was provided to DASH;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for holding data (where the organisation relies on its legitimate interests as a reason for holding data);
- stop collecting and erase data if collecting it is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data

5.2 To ask the Organisation to take any of these steps, the individual should send the request to the Data Protection Officer, by way of notice to the DASH club office.

6. Data Security

6.1 We take the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees, contractors, volunteers or Board members in the proper performance of their duties.

6.2 Where DASH engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7. Impact Assessments

7.1 Some of the work that DASH carries out may result in risks to privacy. Where using that data would result in a high risk to individual's rights and freedoms, we will carry out a data protection impact assessment to determine the necessity and proportionality of this use. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8. Data Breaches

8.1 If DASH discovers that there has been a breach of personal data that poses a significant risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about likely consequences and the mitigation measures DASH has taken.

9. International Data Transfers

9.1 We will not transfer HR-related personal data to countries outside the EEA.

10. Individual Responsibilities

10.1 You are responsible for helping DASH keep personal data up to date. You should let us know if personal information provided to us changes, for example if you move to a new house or change personal requirements.

10.2 You may have access to the personal data of other individuals and of clients in the course of your use of the DASH Club, your employment or contract or volunteer period with DASH. Where this is the case, DASH relies on you to help meet our data protection obligations to all individuals.

10.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

10.4 Further details about the Organisation's security procedures can be found in our Data Security policy.

10.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with in accordance with relevant DASH policies and legislation. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal.