SMASH
ONE PERSON CAN CHANGE A LIFE

Data Protection Policy

1. About this policy

1.1. The policy together with the documents referred to within it set out how we comply with our data protection obligations. Its purpose is also to ensure that all staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.2. Breaches of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

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

2. Our Obligations

2.1. We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information, and how (and when) we delete that information once it is no longer required.

2.2. We will comply with the following data protection principles when processing personal information:

a) we will process personal information lawfully, fairly and in a transparent manner;

b) we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

c) we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

d) we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

e) we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

f) we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

2.3. The CEO is responsible for data protection compliance within the company. If you have any questions or comments about the content of this policy or if you need further information, you should contact the CEO

3. Definitions

criminal offence information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4. Basis for processing personal information

4.1. In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

a) review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(i) that the data subject has consented to the processing;

(ii) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(iii) that the processing is necessary for compliance with a legal obligation to which we are subject;

(iv) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;

(v) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

(vi) that the processing is necessary for the purposes of our legitimate interests or the legitimate interests of a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 4.2 below.

b) except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis;

c) document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

d) include information about both the purposes of the processing and the lawful basis for it in our relevant privacy policy/policies or notice(s);

e) where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 5.2.b) below), and document it; and

f) where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

4.2. When determining whether our legitimate interests are the most appropriate basis for lawful processing, we will:

a) conduct a legitimate interests assessment ('**LIA**') and keep a record of it, to ensure that we can justify our decision;

b) if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment ('**DPIA**');

c) keep the LIA under review, and repeat it if circumstances change; and

d) include information about our legitimate interests in our relevant privacy policies or notice(s).

5. Sensitive personal information

5.1. Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

5.2. We may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

a) we have a lawful basis for doing so as set out in paragraph 4.1 above; and

b) one of the special conditions for processing sensitive personal information applies, e.g.:

(i) the data subject has given has given explicit consent;

(ii) the processing is necessary for the purposes of exercising the employment law rights or obligations of us or the data subject;

(iii) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(iv) processing relates to personal data which are manifestly made public by the data subject;

(v) the processing is necessary for the establishment, exercise or defence of legal claims; or

(vi) the processing is necessary for reasons of substantial public interest.

5.3. Before processing any sensitive personal information, staff must notify the CEO of the proposed processing, in order that the CEO may assess whether the processing complies with the criteria noted above.

6. Data protection impact assessments (DPIAs)

6.1. Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where we are planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

a) whether the processing is necessary and proportionate in relation to its purpose;

b) the risks to individuals; and

c) what measures can be put in place to address those risks and protect personal information.

6.2. Before any new form of technology is introduced, the manager responsible should therefore contact the CEO in order that a DPIA can be carried out.

7. Documentation and records

7.1. We will keep written records of processing activities.

7.2. We will conduct regular reviews of the personal information we process and update our documentation accordingly.

8. Privacy policies / notices

8.1. We will issue privacy policies or notices from time to time, informing data subjects about the personal information that we collect and hold relating to them, how data subjects can expect their personal information to be used and for what purposes.

8.2. We will take appropriate measures to provide information in privacy policies or notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

9. Individual rights

9.1. Data subjects have the following rights in relation to their personal information:

a) to be informed about how, why and on what basis that information is processed. This information is set out in our various privacy policies or notices for staff, candidates and clients;

b) to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request—see our subject access request policy;

c) to have data corrected if it is inaccurate or incomplete;

(i) to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

(ii) to object to the processing of personal information.

d) to restrict the processing of personal information; and

e) to request the transfer of their personal information to another party.

10. Staff obligations

10.1. All staff are responsible for helping us keep their personal information up to date. You should let the HR department know if the information you have provided to us changes, for example if you move house or change details of the bank or building society account to which you are paid.

10.2. During the course of your employment or engagement, you may have access to the personal information of other members of staff, candidates, suppliers, customers and clients. If so, we expect you to help us meet our data protection obligations to those individuals.

10.3. If you have access to personal information, you must:

a) only access the personal information that you have authority to access, and only for authorised purposes;

b) only allow other members of our staff to access personal information if they have appropriate authorisation;

c) only allow individuals who are not members of our staff to access personal information if you have specific authority to do so from the CEO

d) only process the personal information in accordance with this policy;

e) keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in our systems and data security policy);

f) not remove personal information, or devices containing personal information (or which can be used to access it), from our premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device and you have consent to do so from the CEO and

g) not store personal information on local drives or on personal devices that are used for work purposes.

10.4. All staff must read, understand and comply with the provisions of this policy and our other rules, policies and procedures relating to data protection. This includes but is not limited to:

a) Privacy policies or notices in relation to Staff, Mentors, Volunteers, Trustees and other third parties;

b) Our Subject Access Request Procedure;

c) Our Data Management Procedure and Data Map

d) Our Data Correction Procedure

e) Our lone working Policy

f) Our Breach / Incident Reporting Procedure

g) Our Safeguarding Policy

10.5. You should contact CEO if:

a) you receive a request from anyone in relation to the individual rights set out in paragraph 9 above

b) you are concerned or suspect that any aspect of this policy has been breached or is likely to be breached.

11. Information security

11.1. We will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

11.2. Where we use external organisations to process personal information on our behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

a) the organisation may act only on our written instructions;

b) those processing the data are subject to a duty of confidence;

c) appropriate measures are taken to ensure the security of processing;

d) sub-contractors are only engaged with our prior consent and under a written contract;

e) the organisation will assist us in providing subject access and allowing individuals to exercise their rights in relation to data protection;

f) the organisation will assist us in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

g) the organisation will delete or return all personal information to us as requested at the end of the contract; and

h) the organisation will submit to audits and inspections, provide us with whatever information we need to ensure that we are both meeting our data protection obligations, and tell us immediately if it is asked to do something infringing data protection law.

11.3. Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the CEO

12. Retention of personal information

12.1. Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow our data management policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult CEO. Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

13.International transfers

13.1. Actual or possible transfers of personal information outside the European Economic Area ('**EEA**'), must only take place if:

a) The transfer is clearly set out in the relevant privacy policy; and

b) The country in question is either designated as having an adequate level of protection or the organisation has provided adequate safeguards.

13.2. Staff dealing with possible transfers of personal information outside of the EEA must ensure the transfer is covered by the relevant privacy policy or notice and should seek guidance from the CEO

If you have any questions about this policy, please contact the CEO

I,_____
employee/worker/contractor (name), acknowledge that on _____ (date), I received a copy of SMASH's Data Protection Policy and that I have read and understood it.

Signature

……

Name

……