Scottish Society of Botanical Artists

Data Protection Policy

Contents

1. Overview

1.1 The Scottish Society of Botanical Artists (SSBA) takes the security and privacy of personal data and information seriously. As part of our normal course of business we gather and use personal information about a variety of people including members, former members, office-holders, arts venues and other organizations and people who are in general contact with us. The Data Protection Act 2018 (the "2018 Act") and the EU General Data Protection Regulation ("GDPR") regulate the way in which personal information about living individuals is collected, processed, stored or transferred.

1.2 This policy explains the provisions that we will adhere to when any personal data belonging to or provided by data subjects, is collected, processed, stored or transferred on behalf of the SSBA. We expect everyone processing personal data on behalf of the SSBA (see paragraph 5 for a definition of "processing") to comply with this policy in all respects.

1.3 The SSBA has a separate Privacy Notice, called our Privacy Statement, which outlines the way in which we use personal information provided to us. A copy can be obtained from the Secretary (see below).

1.4 All personal data must be held in accordance with the SSBA's Data Retention Policy, which must be read alongside this policy. A copy of the Data Retention Policy can be obtained from the Secretary. Data should only be held for as long as necessary for the purposes for which it is collected.

1.5 This policy does not form part of any contract of employment or contract for services if relevant and can be amended at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the SSBA intends to comply with the 2018 Act and the GDPR.

1.6 The SSBA currently has no employees. Any deliberate or negligent breach of this policy by an employee may result in disciplinary action being taken in accordance with disciplinary procedures. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see Paragraph 12 below) and such conduct by an employee would amount to gross misconduct which could result in dismissal.

2. Data Protection Principles

If processed, personal data will be processed in accordance with the '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;

- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to demonstrate compliance.

3. Definition of personal data

3.1. "Personal data" means information which relates to a living person (a "data subject") who can be identified from that data on its own, or when taken together with other information which is likely to come into the possession of the data controller. It includes any expression of opinion about the person and an indication of the intentions of the data controller or others, in respect of that person. It does not include anonymised data.

3.2. This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

4. Definition of special category personal data

4.1. **'Special category personal data'** is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic or biometric data; data concerning health or health status; or data concerning a person's sex life and sexual orientation.

4.2. No personal data held by SSBA is expected to be classed as special category personal data, either specifically or by implication, in particular information relating to health and health status.

5. Definition of processing

'**Processing'** means any operation which is performed on personal data, such as collection, recording, organisation, structuring or storage; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; and restriction, destruction or erasure.

6. How personal data should be processed

6.1. Everyone who processes data on behalf of the SSBA has responsibility for ensuring that the data they collect and store is handled appropriately, in line with this policy, our Data Retention policy and our Privacy Statement.

6.2. Personal data should only be accessed by those who need it for the work they do for or on behalf of the SSBA. Data should be used only for the specified lawful purpose for which it was obtained.

6.3. The legal bases for processing personal data (other than special category data, which is referred to in Paragraph 8 below) are that the processing is necessary for the purposes of the SSBA's legitimate interests; or that it is necessary to exercise the rights and obligations of the SSBA at law; or that (in relation to the processing of personal data relating to criminal convictions and offences or related security measures) the processing meets a condition in Part 1, 2 or 3 of Schedule 1 of the 2018 Act.

6.4. Personal data held in all ordered manual files and databases should be kept up to date. It should be shredded or disposed of securely when it is no longer needed. Unnecessary copies of personal data should not be made.

7. Privacy Statement

7.1. If someone may not reasonably expect the way in which we use their personal data, we will issue information about this using a Privacy Notice (our Privacy Statement) which will be given to them when the data is provided or on request.

7.2. If our use of personal data is what someone would reasonably expect, we will provide information about this using our Privacy Statement which is obtainable from the SSBA.

8. When is consent needed for the processing of personal data?

8.1. It is expected that in all cases the individual will have given explicit consent to the processing of the personal data for one or more specified purposes.

8.2. The relatively small amount of this processing carried out by SSBA will be carried out by SSBA with appropriate safeguards to keep information safe and secure. This information will not be disclosed outside SSBA without consent, per paragraph 8.1.

8.3. Where personal data is to be shared with a third party, the SSBA will only do so with the explicit consent of the data subject. For example, personal data will only be included in a directory for circulation where consent has been obtained.

8.4. If consent is required to process the information this should be recorded using the consent forms available from the Secretary. If consent is given orally rather than in writing, this fact should be recorded in writing.

9. Keeping personal data secure

9.1. Personal data should not be shared with those who are not authorised to receive it. Care should be taken when dealing with any request for personal information over the telephone or otherwise. Identity checks should be carried out if giving out information to ensure that the person requesting the information is either the individual concerned or someone properly authorised to act on their behalf.

9.2. Hard copy personal information should be stored securely (in lockable storage, where appropriate) and not visible when not in use. Filing cabinets and drawers and/or office doors should be locked when not in use. Keys should not be left in the lock of the filing cabinets/lockable storage.

9.3. Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.

9.4. Sending or receiving Emails containing personal information at a work email address should be avoided as this might be accessed by third parties.

9.5. The 'bcc' rather than the 'cc' or 'to' fields should be used when emailing a large number of people, unless everyone has agreed for their details to be shared amongst the group.

9.6. Wherever practicable, personal data should be encrypted or password-protected before being transferred electronically.

9.7. Personal data should never be transferred outside the European Economic Area except in compliance with the law.

10. Sharing personal data

10.1. We will only share someone's personal data where we have a legal basis to do so, including for our legitimate interests, and any personal data (and its processing basis) will be maintained and kept up to date. This may require information relating to health or health status, with appropriate consent.

10.2. We will not send any personal data outside the United Kingdom. If this changes all individuals affected will be notified and the protections put in place to secure your personal data, in line with the requirements of the GDPR, will be explained.

11. How to deal with data security breaches

11.1. Should a data security breach occur, the SSBA member will notify the SSBA secretary immediately. If the breach is likely to result in a risk to the rights and freedoms of individuals then the Information Commissioner's Office must be notified within 72 hours.

11.2. Breaches will be handled by the relevant office holder in accordance with the SSBA's data security breach management procedure.

12. Subject access requests

12.1. Data subjects can make a subject access request to find out what information is held about them. This request must be made in writing. Any such request received by the SSBA should be forwarded immediately to the Secretary or Chair who will coordinate a response within the necessary time limit (within a reasonable time or within 30 days at most).

12.2. It is a criminal offence to conceal or destroy personal data which is part of a subject access request.

13. Data subject rights

13.1. Data subjects have certain other rights under the GDPR. This includes the right to know what personal data the SSBA processes, how it does so and what the legal basis is for doing so.

13.2. Data subjects also have the right to request that the SSBA corrects any inaccuracies in their personal data, and erase their personal data where the SSBA is not entitled by law to process it or it is no longer necessary to process it for the purpose for which it was collected. Data should be erased when an individual revokes their consent (and consent is the basis for processing); when the purpose for which the data was collected is complete; or when compelled by law.

13.3. All requests to have personal data corrected or erased should be passed to an officer of the SSBA who will liaise with either the Secretary or the Chair or both, who are jointly responsible for the SSBA response and any supervising action to be taken.

14. Policy review

SSBA management will be responsible for reviewing this policy from time to time and updating its data protection responsibilities and any risks in relation to the processing of data.

For information, contact the SSBA Secretary, by e-mailing secretary@thessba.org.