Outside In

Policy: Data Protection

Date agreed by Governance Board: ***May 2018***
Review Date: Annually

Policy statement

Outside In is a national project providing a platform for artists to access the art world who may find it difficult due to health, disability, social circumstance or isolation.

This policy is designed to ensure that all staff are aware of their particular responsibilities in relation to the Data Protection Act 1998 (the 'Act'), the General Data Protection Regulation EU 2016/679 ('GDPR') and other regulations (in each case, as updated and amended from time to time) and their associated codes of practices (together, the 'Data Protection Legislation'); and to inform members of the public how Outside In complies with the legislation. It is also to minimise the risk of Outside In breaching the Data Protection Legislation; thereby potentially damaging valued relationships with staff; supporters; and other audiences as well as its reputation.

Once read, please sign the register that your line manager has on record to show that you have understood the policy.

Contents

1 Policy Statement

1.1 During the course of our activities we will collect, store and process personal data about our artists, supporters and other individuals with whom we communicate. We recognise that the fair, transparent and lawful treatment of this data will maintain confidence in our organisation.

1.2 Data users and data processors must comply with, and behave in manner that facilitates our compliance with, this policy when processing personal data on our behalf. Any breach of this policy by our employees may result in disciplinary action.

2 About this Policy

2.1 The types of personal data that we may be required to handle include information about current, past and prospective staff, visitors, supporter, artists and others that we communicate with. The personal data is subject to certain legal safeguards (the **Data Protection Legislation**) which are specified in the Data Protection Act 1998 and other regulations, and which shall, from 25 May 2018, be specified in the General Data Protection Regulation and other regulations.

2.2 This policy, together with any other documents referred to herein, sets out the basis on which we will process personal data, and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

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

2.4 The Outside In Communications Coordinator is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Communications Coordinator

3 Definition of Data Protection Terms

3.1 **Data subjects**, for the purpose of this policy, include all living individuals about whom we hold personal data.

3.2 **Personal data** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.3 **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. We (Outside In) are the data controller of all personal data used in our organisation for our own purposes and for the purposes of processing personal data pursuant to this policy.

3.4 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.5 **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on our behalf and on our instructions, and which is not a data user.

3.6 **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.7 **Sensitive personal data** is a special category of personal data, including information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4 Data Protection Principles

All persons who process personal data under this policy must comply with the principles of good practice. These provide that personal data must be:

(a) processed fairly, lawfully, and in a transparent manner in relation to data subjects;

(b) processed for limited purposes only;

(c) adequate, relevant and limited to what is necessary for the purposes for which it is processed;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which permits identification of data subjects for no longer than necessary for the purpose for which the personal data is processed;

(f) processed in line with data subjects' rights;

(g) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and

(h) not transferred to people or organisations situated in countries without adequate protection.

5 Fair and Lawful Processing

5.1 For personal data to be processed lawfully, one of the legal grounds set out in the Data Protection Legislation must apply. We shall only process personal data if:

(a) the data subject has consented to processing;

(b) processing is necessary in order to perform a contract with the data subject;

(c) processing is necessary to comply with a legal obligation to which we are subject;

(d) processing is necessary to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest; or

(f) processing is necessary for the purposes of the legitimate interest of the data controller or the party to whom the data is disclosed (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject).

5.2 We shall ensure that any overseas transfer of personal data is governed by appropriate transfer mechanisms (for example, contractual protections requiring the data processor to keep personal data secure). Data users should consult with the Communications Coordinator when dealing with commercial discussions with data processors. If a data processor uses a subcontractor, the data processor must be liable for the acts/omissions of the subcontractor.

5.3 When sensitive personal data is being processed, additional conditions must be met, including receiving explicit consent from the data subject, and we shall ensure that such conditions are met when we are processing personal data as data controllers in the course of our activities.

6 Processing for Limited Purposes

Whenever we collect personal data, it must be for a specific and legitimate purpose, which shall be notified to the data subject in accordance with paragraph 7.

7 Notifying Data Subjects

7.1 Where we collect personal data directly from data subjects, we shall inform the data subject of:

(a) the purpose or purposes and legal basis for which we intend to process that personal data;

(b) if applicable, the legitimate interest pursued in accordance with paragraph 5.1(f);

(c) the types of third parties, if any, with which we will share or to which we will disclose that personal data;

(d) if applicable, the fact that we intend to transfer such personal data overseas, together with a reference to the applicable safeguard and the means by which to obtain a copy of them or where they have been made available;

(e) the period for which such personal data shall be stored or, if that is not possible, the criteria for determining such period;

(f) the existence of the data subject's rights which are listed in paragraphs 8.3 and 11;

(g) where processing is based on data subject consent, the right for the data subject to withdraw consent at any time;

(h) the right to lodge a complaint with a supervisory authority;

(i) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and -

(j) the existence of any automated decision-making, which produces legal effects concerning the data subject or similarly affects the data subject, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

7.2 If we receive personal data about a data subject from other sources, we shall provide the data subject with the information in paragraph 7.1 above, together with details of the categories of personal data concerned and the source of the personal data (and, if applicable, whether it came from a public source), as soon as possible thereafter.

7.3 We shall also inform data subjects whose personal data we process that we are the data controller with regard to that data.

7.4 If we intend to further process the personal data for a purpose other than that for which the personal data was collected, we shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 7.1.

8 Consent

8.1 Where processing is based on consent, we must be able to demonstrate that the data subject has consented to processing of his or her personal data.

8.2 If the data subject's consent is given in the context of a written declaration which also concerns other matters, we shall present the request for consent in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

8.3 The data subject shall have the right to withdraw his or her consent at any time. Data users should consult with the Communications Coordinator if they receive a notification that a data subject wishes to withdraw his or her consent.

8.4 When assessing whether consent is freely given by the data subject, utmost account shall be taken of whether, amongst other things, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

9 Accurate Data

We shall ensure that personal data we hold is accurate and kept up to date. We shall check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We shall take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10 Minimal Processing

10.1 We shall only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

10.2 We shall not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We shall not further process data in a manner which is incompatible with the purpose or purposes for which it was collected. We shall take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

10.3 We shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation in an effective manner and integrate the necessary safeguards into the processing in order to meet the requirements of the Data Protection Legislation and protect the rights of data subjects.

10.4 We shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed. That obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility. In particular, such measures shall ensure that by default personal data is not made accessible without the individual's intervention to an indefinite number of natural persons.

11 Processing in line with Data Subject's Rights

We shall process all personal data in line with data subjects' rights, in particular their right to:

(a) request access to any data held about them by a data controller (see also paragraph 16);

(b) prevent the processing of their data for direct-marketing purposes;

(c) ask to have inaccurate data amended (see also paragraph 9);

(d) prevent processing that is likely to cause damage or distress to themselves or anyone else;

(e) have personal information erased;

(f) not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (unless an exception in the Data Protection Legislation applies and the data subject has had opportunity to contest such decision); and

(g) receive personal data held about them in a commonly used, machine-readable format, and have the personal data transmitted directly from one data controller to another where it is technically feasible.

12 Data Security

12.1 We shall take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

12.2 We shall put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data shall only be transferred to data processors if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

12.3 We shall maintain data security by protecting 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 processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

12.4 Security procedures include:

(a) **Entry controls.** Any unfamiliar person 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. Digital storage devices should be physically destroyed or wiped when they are no longer required.

(d) **Equipment.** Data users must 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.

13 Data Processors

13.1 We shall only use processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the data subject.

13.2 Our contracts with data processors shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

13.3 Our contracts with data processors shall stipulate that the processor:

(a) processes the personal data only on our documented instructions;

(b) ensures that persons authorised to process the personal data are subject to appropriate confidentiality obligations;

(c) takes all measures required to ensure the security of the personal data;

(d) shall not engage another processor without our prior written consent, and where another processor is engaged, it must be subject to obligations equal to obligations imposed on the original processor, and the original processor must remain fully liable to us for performance of its data protection obligations;

(e) assists us by using appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of our obligation to respond to requests for exercising the data subject's rights;

(f) assists us to comply with our obligations under the Data Protection Legislation;

(g) shall, at our discretion, delete or return personal data at the end of the service provision (unless required by law to store the personal data);

(h) makes available to us all information necessary to demonstrate its compliance with its data protection obligations in its contract with us; and

(i) shall keep a written record (which may be in electronic form) of all processing activities, which it shall make available to a supervisory authority on request, containing the following information:

(i) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(ii) the categories of processing carried out;

(iii) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if applicable, the documentation of appropriate safeguards; and

(iv) where possible, a general description of the technical and organisational security measures which are in place to protect personal data.

14 Transferring Personal Data to a Country Outside the EEA

14.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms;

(b) the data subject has given his/her consent;

(c) the transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject;

(d) the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or

(e) the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

14.2 Subject to the requirements in paragraph 14.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15 Disclosure and Sharing of Personal Information

15.1 We may share personal data we hold with anyone working for Outside In Art Charitable Incorporated Organisation, known as Outside In, and with authorised personnel within our regional partners.

15.2 We may disclose personal data we hold to third parties if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, supporters, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

15.3 We may share personal data with data processors in accordance with the terms of this policy.

15.4 We may share personal data we hold with selected third parties upon obtaining appropriate consent of the data subject.

16 Dealing with Subject Access Requests

16.1 Data subjects may make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Communications Coordinator immediately.

16.2 When receiving telephone enquiries, we shall only disclose personal data we hold on our systems if we verify the caller's identity to make sure that information is only given to a person who is entitled to it. If we are not sure about the caller's identity and where their identity cannot be checked and we shall suggest that the caller put their request in writing.

16.3 Data users shall refer a request to the Communications Coordinator for assistance in difficult situations. Data users should not be bullied into disclosing personal information.

16.4 Where the request for information is made in electronic form, we shall provide the information in electronic form where possible, unless otherwise requested by the data subject.

16.5 We shall deal with requests for information without undue delay. Within one month of a request for information, we shall either:

(a) provide the information to the data subject;

(b) if the complexity or number of requests requires, extend the response period by up to a further two months and inform the data subject of such extension; or,

(c) not action the information request, and inform the data subject of the reason for not taking action and of the possibility for lodging a complaint or seeking a judicial remedy.

16.6 If requests for information are manifestly unfounded or excessive (particularly if they are repetitive), we may charge a reasonable fee to carry out the request or refuse to action the request. Employees who suspect they have received such requests should refer them to the Communications Coordinator. Otherwise, initial requests shall be dealt with free of charge, and we may charge a reasonable fee for further requests.

17 Changes to this Policy

We reserve the right to change this policy at any time. Where appropriate, we shall notify subjects of this policy of those changes through our website.

18 Management of this Policy

18.1 The Director, managers, staff and volunteers are responsible for ensuring that the Data Protection policy is adhered to.

18.2 OI's Director will review this policy annually.