DATA PROTECTION POLICY

Date Issued: 15th September 2022
Date Reviewed: 5th July 2023

Next Review Date: 5th July 2024

Trustee signature: 

Trustee Full Name: NINA LEMON

Trustee Full Name: CAROLINE HOARE

Peer Productions needs to keep certain information about its employees, students, project participants and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safety and not disclosed to any other person unlawfully. To do this, Peer Productions must comply with the Data Protection Principles which are set out in the Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation

1. INTRODUCTION

1.1 Peer Productions, "the Charity" is the Data Controller for the purposes of the EU General Data Protection Regulation.

1.2 The Charity collects and uses certain types of personal information about the following categories of individuals, for the types of information and what we do with it, please see paragraph 11.1 below:

1.2.1 Staff;

1.2.2 Volunteer actors;

1.2.3 Trustees;

1.2.4 Service users and participants;

1.2.5 Beneficiaries;

1.2.6 Donors;

1.2.7 Suppliers;

1.2.8 Service purchasers including schools;

1.2.9 People who download our Teachers' Packs;

1.2.10 People who fill in our surveys;

1.2.11 Freelance workshop leaders;

1.2.12 Professional writers,actors and other artists;

1.2.13 Children and young people involved in our events; and

1.2.14 Next of kin of our volunteers, participants and service users.

1.3 The Charity will process this personal information in the following ways:

1.3.1 to ensure that we can provide an effective service to our clients and service users;

1.3.2 to comply with statutory and contractual obligations relating to employment; and

1.3.3 to comply with statutory and other legal obligations relating to safeguarding.

1.4. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the EU General Data Protection Regulation (the "GDPR") and other related legislation. It will apply to information regardless of the way it is used or recorded and applies for as long as the information is held.

1.5. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.6. This policy will be updated as necessary to reflect best practice, or amendments made to the GDPR, and shall be reviewed every 12 months.

2. PERSONAL DATA

2.1. 'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain (for example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.) A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

2.1.1 race or ethnic origin;

2.1.2 political opinions;

2.1.3 religious or philosophical beliefs;

2.1.4 trade union membership;

2.1.5 physical or mental health;

2.1.6 an individual's sex life or sexual orientation;

2.1.7 genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

3. THE DATA PROTECTION PRINCIPLES

3.1. The six data protection principles as laid down in the GDPR are followed at all times:

3.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

3.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/ those purposes;

3.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2. In addition to this, the Charity is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 9 and 10 below).

3.3. The Charity is committed to complying with the principles in 3.1 at all times. This means that the Charity will:

3.3.1 inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

3.3.2 be responsible for checking the quality and accuracy of the information;

3.3.3 regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Data Retention Policy;

3.3.4 ensure that when information is authorised for disposal it is done appropriately;

3.3.5 ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

3.3.6 share personal information with others only when it is necessary and legally appropriate to do so;

3.3.7 set out clear procedures for responding to requests for access to personal information known as subject access requests;

3.3.8 report any breaches of the GDPR in accordance with the procedure in paragraph 13 below.

4. CONDITIONS FOR PROCESSING PERSONAL INFORMATION

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

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

4.2.1 that the data subject has consented to the processing;

4.2.2 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;

4.2.3 that the processing is necessary for compliance with a legal obligation to which the Charity is subject;

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

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

4.2.6 that the processing is necessary for the purposes of legitimate interests of the Charity or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

4.3 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

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

4.5 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

4.6 where sensitive personal information is processed, also identify a lawful special condition for processing that information and document it; and

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

4.8 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

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

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

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

4.8.4 include information about our legitimate interests in our relevant privacy 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 The Charity may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

5.2.1 we have a lawful basis for doing so as set out in paragraph 4.2 above, e.g. it is necessary for the performance of the employment contract, to comply with the Charity's legal obligations or for the purposes of the Charity's legitimate interests; and

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

5.2.3 the data subject has given has given explicit consent;

5.2.4 the processing is necessary for the purposes of exercising the employment law rights or obligations of the Charity or the data subject;

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

5.2.6 processing relates to personal data which are manifestly made public by the data subject;

5.2.7 the processing is necessary for the establishment, exercise or defence of legal claims; or

5.2.8 the processing is necessary for reasons of substantial public interest.

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

5.4 Sensitive personal information will not be processed until:

5.4.1 the assessment referred to in paragraph 5.2 has taken place; and

5.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

5.5 The Charity will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

5.6 In relation to sensitive personal information, the Charity will comply with the procedures set out in paragraphs 5.7 and .5.8 below to make sure that it complies with the data protection principles set out in paragraph 3 above.

5.7 **During the recruitment process**: the Charity, with guidance from the Strategy & Partnerships Director, will ensure that (except where the law permits otherwise):

5.7.1 during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;

5.7.2 if sensitive personal information is received, e.g. the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

5.7.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

5.7.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

5.7.5 we will only ask health questions where required once an offer of employment has been made.

5.8 **During employment**: the Charity, with guidance from the Strategy & Partnerships Director, will process:

5.8.1 health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

5.8.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting**.** Where possible, this information will be anonymised; and

5.8.3 trade union membership information for the purposes of staff administration and administering 'check off'.

6. DISCLOSURE OF PERSONAL DATA

6.1 The following list includes the most usual reasons that the Charity will authorise disclosure of personal data to a third party:

6.1.1 to give a confidential reference relating to a current or former employee, or volunteer;

6.1.2 for the prevention or detection of crime;

6.1.3 for the assessment of any tax or duty;

6.1.4 where it is necessary to exercise a right or obligation conferred or imposed by law upon us (other than an obligation imposed by contract)

6.1.5 for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

6.1.6 for the purpose of obtaining legal advice;

6.1.7 for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

6.2 The Charity may receive requests from third parties (i.e. those other than the data subject, the Charity, and its employees) to disclose personal data it holds about individuals. This information will not generally be disclosed unless one of the specific exemptions under the GDPR which allow disclosure applies, or where disclosure is necessary for the legitimate interests of the third party concerned or the Charity.

6.3 All requests for the disclosure of personal data must be sent to Strategy & Partnerships Director, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the requesting third party before making any disclosure.

7. INTERNATIONAL TRANSFERS

7.1 The Charity may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) on the basis that that country, territory or organisation is designated as having an adequate level of protection or has provided adequate safeguards by way of binding corporate rules or by some other acceptable means.

8. SECURITY OF PERSONAL DATA

8.1 The Charity will take reasonable steps to ensure that members of staff and volunteers will only have access to personal data where it is necessary for them to carry out their duties. All staff and volunteers will be made aware of this Policy and their duties under the GDPR. The Charity will

take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

8.2 For further details as regards security of IT systems, please refer to the ICT Policy.

9. SUBJECT ACCESS REQUESTS

9.1 Anybody who makes a request to see any personal information held about them by the Charity is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see paragraph 1.5).

9.2 All requests should be sent to the Strategy & Partnerships Director within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt unless there are grounds to extend the period of compliance by a further 2 months, in which case the Charity will inform the individual of the extension within one month of receipt and explain why the extension is necessary.

9.3 Where a child or individual does not have sufficient understanding to make their own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Strategy & Partnerships Director must, however, be satisfied that:

9.3.1 the child or individual lacks sufficient understanding; and

9.3.2 the request made on behalf of the child or individual is in their interests.

9.4 Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Charity must have written evidence that the individual has authorised the person to make the application and the Strategy & Partnerships Director must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

9.5 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

9.6 A subject access request must be made in writing. The Charity may ask for any further information reasonably required to locate the information.

9.7 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent

would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

9.8 All files must be reviewed by Strategy & Partnerships Director before any disclosure takes place. Access will not be granted before this review has taken place.

9.9 Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

10. OTHER RIGHTS OF INDIVIDUALS

10.1 All individuals have the following rights in relation to their personal information:

10.1.1 to be informed about how, why and on what basis that information is processed;

10.1.2 to have data corrected if it is inaccurate or incomplete;

10.1.3 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’);

10.1.4 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased), or where the Charity no longer needs the personal information but the individual requires the data to establish, exercise or defend a legal claim; and

10.1.5 to restrict the processing of personal information temporarily where the individual does not think it is accurate (and the Charity is verifying whether it is accurate), or where the individual has objected to the processing (and the Charity is considering whether the organisation’s legitimate grounds override your interests).

10.2 If you wish to exercise any of the rights set out above, please contact the Strategy & Partnerships Director.

11. EXEMPTIONS TO ACCESS

11.1 In certain circumstances the Charity may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

11.2 **Crime detection and prevention:** We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we are able to. For example, if the disclosure of the personal data could alert the individual to the fact that he or she is being investigated for an illegal activity (i.e. by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

11.3 **Protection of rights of others:** We do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information (or that information and any other information that we reasonably believe the data subject is likely to possess or obtain), unless:

11.3.1 that other individual has consented to the disclosure of the information to the individual making the request; or

11.3.2 it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:

11.3.3 the type of information that would be disclosed;

11.3.4 any duty of confidentiality owed to the other individual;

11.3.5 any steps taken by the controller with a view to seeking the consent of the other individual;

11.3.6 whether the other individual is capable of giving consent; and

11.3.7 any express refusal of consent by the other individual.

11.4 **Confidential references:** We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

11.4.1 education, training or employment of the individual;

11.4.2 appointment of the individual to any office; or

11.4.3 provision by the individual of any service

11.5 This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means you must consider the rules regarding disclosure of third-party data before disclosing the reference.

11.6 **Legal professional privilege:** We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

11.6.1 'Advice privilege' covers confidential communications between the Charity and our lawyers where the dominant purpose of the communication is the seeking or giving of legal advice;

11.6.2 'Litigation privilege' covers any document which was created with the dominant purpose of being used in actual or anticipated litigation (e.g. legal proceedings before a court or tribunal). Once a bona fide claim to litigation privilege ends, the documents in the file which were subject to litigation privilege become available if a data subject access request is received.

11.7 If you think the legal professional privilege exemption could apply to the personal data that have been requested, you should refer the matter to the Strategy & Partnerships Director for further advice.

11.8 **Management forecasting:** We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions and demotions. This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

11.9 **Negotiations:** We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

12. INDIVIDUAL OBLIGATIONS

12.1 Charity staff may have access to the personal information of other members of staff, donors, suppliers, service users and other third parties in the course of their employment or engagement. If so, the Charity expects them to help meet its data protection obligations to those individuals.

12.2 All those with access to personal information, must:

12.2.1 only access the personal information that they have authority to access, and only for authorised purposes;

12.2.2 only allow other Charity staff to access personal information if they have appropriate authorisation;

12.2.3 only allow individuals who are not Charity staff to access personal information if they have specific authority to do so from the Strategy & Partnerships Director;

12.2.4 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 the Charity's ICT Policy.

12.3 Staff should contact the Strategy & Partnerships Director if they are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.3.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 4.2 being met;

12.3.2 any data breach as set out in paragraph 13 below;

12.3.3 access to personal information without the proper authorisation;

12.3.4 personal information not kept or deleted securely;

12.3.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Charity's premises without appropriate security measures being in place;

12.3.6 any other breach of this policy or of any of the data protection principles.

13. BREACH OF ANY REQUIREMENT OF THE GDPR

13.1 Any and all breaches of the DPA, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to Strategy & Partnerships Director, in accordance with paragraph 12 above.

13.2 Once notified, the Strategy & Partnerships Director shall assess:

13.2.1 the extent of the breach;

13.2.2 the risks to the data subjects as a consequence of the breach;

13.2.3 any security measures in place that will protect the information;

13.2.4 any measures that can be taken immediately to mitigate the risk to the individuals.

13.3 Unless the Strategy & Partnerships Director concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Charity, unless a delay can be justified.

13.4 The Information Commissioner shall be told:

13.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects;

13.4.2 the contact point for any enquiries (which shall usually be Strategy & Partnerships Director);

13.4.3 the likely consequences of the breach;

13.4.4 measures proposed or already taken to address the breach.

13.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Strategy & Partnerships Director shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

13.6 Data subjects shall be told:

13.6.1 the nature of the breach;

13.6.2 who to contact with any questions;

13.6.3 measures taken to mitigate any risks.

13.7 The Strategy & Partnerships Director shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Board and a decision made about implementation of those recommendations.

14. CONSEQUENCES OF FAILING TO COMPLY

14.1 The Charity takes compliance with this policy very seriously. Failure to comply with this policy:

14.1.1 puts at risk the individuals whose personal information is being processed;

14.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Charity; and

14.1.3 may, in some circumstances, amount to a criminal offence by the individual.

14.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect and/or other appropriate action will be taken.

15. TYPES OF DATA AND RETENTION OF DATA

15.1. Please refer to our Data Retention Policy for details of the data we collect, the purpose for which it is processed, and the time periods that different

types of data that must be retained for business and legal purposes are kept for.

16. CONTACT

16.1 If anyone has any concerns or questions in relation to this policy they should contact Strategy & Partnerships Director.