|  |
| --- |
|  |
|  |
|  |

|  |
| --- |
|  |

**Logo

Description automatically generatedARTS DREAM SELSEY (ADS ) DATA PROTECTION POLICY 2018**

**REGISTERED ADDRESS: 6. Sea Grove, Selsey. PO209HT**

**Company number: 8857997**

**Charity number :1155713**

**Email:** [**artsdream@gmail.com**](mailto:artsdream@gmail.com)

**Website :** [**www.artsdream2013selsey.weebly.com**](http://www.artsdream2013selsey.weebly.com)

|  |  |
| --- | --- |
| Policy information | |
| Organisation | Arts Dream Selsey |
| Scope of policy | To Arts Dream Trustees, Management Committee, workshop staff and all users |
| Policy operational date | March 2018 |
| Policy prepared by | Christine Butler. Director Arts Dream Selsey |
| Date approved by Board/ Management Committee |  |
| Policy review date | March 2021 |

1. **Purpose of the policy**

The purpose of this policy is to :

* comply with the law and the Data Protection Act 1988
* follow good practice
* protect clients, staff and other individuals
* protect the organisation

**Data PROTECTION ACT 1988**

The purpose of this policy is to ensure compliance of the Charity with all of its obligations under the Data Protection Act 1998. The policy provides guidance on the maintenance of and access to records as set out in the Act. The Act indicates:

The [Data Protection Act](http://www.legislation.gov.uk/ukpga/1998/29/contents) controls how your personal information is used by organisations, businesses or the government.

Everyone responsible for using data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

* used fairly and lawfully
* used for limited, specifically stated purposes
* used in a way that is adequate, relevant and not excessive
* accurate
* kept for no longer than is absolutely necessary
* handled according to people’s data protection rights
* kept safe and secure
* not transferred outside the [European Economic Area](https://www.gov.uk/eu-eea) without adequate protection

There is stronger legal protection for more sensitive information, such as:

* ethnic background
* political opinions
* religious beliefs
* health
* sexual health
* criminal records

**2.0 Policy Statement :**

2.1 This policy aims to:

* comply with both the law and good practice
* respect individuals’ rights
* be open and honest with individuals whose data is held
* provide training and support for staff who handle personal data, so that they can act confidently and consistently

**3.0 Key Risks**

Arts Dream has identified two main risks within the organisation

* 1. information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information
  2. individuals being harmed through data being inaccurate or insufficient

**4. 0 Data Protection Principles:**

4.1 Personal data shall be processed fairly and lawfully.

4.2 Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

4.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4.4 Personal data shall be accurate and where necessary, kept up to date.

4.5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

4.6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

4.7 Computer based personal data will be stored in accordance with the provisions of the Data Protection Act.

4.8 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

4.9 Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

**5.0 Data Protection Responsibilities:**

**5.1 Data Controller:**

The Chairman of the Board is the Data Controller as defined in the Data Protection Act 1998.

Data management responsibilities have been delegated to the Director of Arts Dream Selsey the trustees, and all the management team

5.2 Data handling responsibilities have been delegated to Christine Butler who will brief the

board and management team on Data Protection responsibilities

* 1. Reviewing Data Protection and related Data Protection issues
  2. Ensuring that Data Protection induction and training takes place
  3. Handling any difficult requests
  4. Approving unusual or controversial disclosures of personal data policies
  5. Advising other staff on any difficult issues

5.8 Data handling responsibilities include but are not limited to:

1. Implementing any policies regarding data protection
2. Ensuring that safe and confidential systems are in place throughout Arts Dream projects and its organisation

5.9 All staff and volunteers should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on where ‘staff’ is used, this includes both paid staff, workshop leaders and volunteers.)

**6. 0 Confidentiality :**

6.1 Scope :

Confidentiality applies to a much wider range of information than Data Protection. Some things within our organisation are confidential. These are likely to be confidential, but may well not be subject to Data Protection. These include :

* Information about the organisation (and its plans or finances, for example)
* Information about other organisations, since Data Protection only applies to information about individuals
* Information which is not recorded, either on paper or electronically
* Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a “relevant filing system” in the Data Protection Act

**6.2 Understanding of confidentiality:**

Normally access will be defined on a “need to know” basis; no one should have access to information unless it is relevant to their work. This may be relaxed in the case of information which poses a low risk: for example a list of business contacts may be made generally available, even if this means people having access who don’t strictly need it.

**6.3 Duty of Data Protection and Confidentiality:**

6.4 Part time staff and volunteers operating within Arts Dream will maintain confidentiality with written or oral information relating to its own staff, committee, volunteers, stakeholders and the wider community.

6.5 In order that personal information is handled according to the requirements of both common law and the Data Protection Act 1998, ADS will maintain the confidentiality of personal information and follow the Charity’s Data Protection Policy and procedures therein.

6.6. All ADS, committee, part time staff and volunteers agree:

* To treat all information about staff, volunteers, stakeholders and the wider community as confidential.
* To adhere to ADS Data Protection Policy and related policies.
* To only disclose personal Information in accordance with this policy.
* That any non-compliance with this Policy will be treated as misconduct and subject to Disciplinary Procedures.
* That all confidential information about ADS that is information not in the public domain, must not be disclosed.
* To maintain this confidentiality even when employment and volunteering has ceased for the protection of the individual.

6.7 *In relation to Marketing:*

6.8 Although the Act does not define direct marketing clearly enough to be certain whether it incorporates many of the activities of voluntary organisations, good practice suggests that most unsolicited direct contact with individuals should be treated as marketing. This would include seeking donations, marketing goods and services, promoting sponsored events, raffles, etc.

6.9. Because Data Subjects have the right to require their data not to be used for marketing, it is good practice to make it clear when there is an intention to use their data for marketing and offer them an opt-out. When we sell things on line and through Face Book there is a built in Opt out, ( people can unlike our FB page)

7.0 ADS has agreed to :

* Share lists with other organisations only where it can be guaranteed that those on the list have been given an opportunity to opt out, and also lists which can be guaranteed to be sufficiently up to date.
* Because of the Data Protection and Privacy (EC Directive) Regulations 2003 most electronic marketing (by phone, fax, e-mail or text message) either requires consent in advance, or it is good practice (and administratively easier) to obtain consent.
* ADS can do this through offering a particular op out clause on all mail outs

**7. 0 Definitions of Data :**

7.1 Personal data is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining or disposing of information.

7.2 The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to information in education records. Examples would be names of staff and clients, dates of birth, addresses, national insurance numbers, assessment results, medical information, SEN assessments, reviews and some minutes of meetings.

7.3 Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sexuality and criminal offences.

7.4 There are greater legal restrictions on processing sensitive personal data than there are on personal data.

**8. 0 Data Types:**

8. 1. This policy covers data transferred by email, written forms, post, fax, text and social media entries or verbally.

6.2 The Trustees. Management team and workshop leaders must :

* Be able, if asked, to justify their sharing of personal information;
* Maintain security to the level expected by the classification of the personal information, whether the sharing is in person, by email, written forms, post, fax, text and social media entries or verbally;
* Not use removable media devices – such as memory sticks to share information, except in instances where this is the most sensible means of sharing where the memory stick must be encrypted with a code or password and where the code or password is shared separately to the memory stick. Codes or passwords should not be written down but memorised.

**9.0 Sharing Data:**

9.1. Personal data requests must be made in writing to the charity and responded to within 28 days of receipt. If the data requested will take longer than 28 days to compile, a holding letter must be sent within 28 days of receipt of the request.

9.1 A charge can be made for the data requested, in line with the costs of the printing, postage and staff time to collate the data. A charge must be reasonable and not be used to discourage a request.

9.2. Before sharing or sending the personal information you must be satisfied:

* Of the **identity of the recipient**; this includes internal colleagues, external third parties and individuals;
* Of the **contact details of the recipient** – e.g. email address, fax number, phone number, address;
* Of the recipient’s **need to know and/or their entitlement to** the personal information, seeking written proof where necessary;
* That they are **authorised** to be in receipt of the sharing of the personal information

Always consider the amount of information you are sharing.

**9.3 Adults requesting access to their child’s data**

**Very few of ADS projects deal with children but we have included information here that may be necessary in future years.**

9.4 A person who has parental responsibility for a child has a right to make decisions about their care and upbringing. The following people automatically have parental responsibility:

* All birth mothers
* Fathers married to the mother at the time the child was born
* Fathers who are not married to the mother but are registered on the child’s birth certificate. The registration or re-registration must have taken place after December 2003.
* Civil partners and partners of mothers registered as the child’s legal parent on the birth certificate.
* Others may require parental responsibility through a court residency or parental responsibility order
* Parental responsibility may be shared with the local authority if the child is subject of a care order

9.5 Automatic right to access is given to those with parental responsibility where the child is up to and including age 11.

9.6 Automatic right to access is not given to those with parental responsibility where the child is age 12 and over. After the age of 11 Fraser Guidelines and Gillick Competency should be applied (see Appendix A).

**9.7 Under 16’s requesting access to their own data:**

9.8. Children under the age of 12 will not have automatic rights to their records. Where a child under the age of 12 requests access to their own records, this must be done in conjunction with a person or persons with parental responsibility.

9.9 Children age 12 and over will not have automatic rights to their records and all children must be compliant with the Gillick Competency and that Fraser Guidelines. (See https://www.nspcc.org.uk )

**10. Disclosure of Information:**

10.1 **EMAIL** - care should be taken when addressing all emails to prevent accidental sharing to unintended recipients

* Each email address should be double checked before pressing send
* Care should be given if the email software auto-completes email addresses
* When sending to more than one person or persons, use BCC so as not to disclose one recipients personal email address to another recipient
* Use the “Delivery Receipt” and “Read Receipt” facilities within the software to ensure delivery and readership by the correct recipient
* Confidential emails should have the word CONFIDENTIAL in capital letters in the heading
* The first paragraph of the email should be the following disclaimer or similar: *The information contained in this email is strictly confidential and is intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this email in error, please notify the sender.*
* Where deemed necessary the “call and confirm” approach should be used, in so much as a follow up telephone call can be made to ensure that the recipient received the email

10.2 **POST** – sensitive personal information, especially regarding health or criminal record (actual or suspected) must be posted by special delivery or recorded delivery OR delivered in person, with the recipient signing to state that they have received the data.

10.3 **VERBALLY** – employees must protect the interests of the individuals subject to their personal information, for example their confidentiality and right to privacy, and the Charity’s interests when

* Discussing personal information in conversations (be sure you are not overheard)
* Using telephones; or
* Recording information on voicemail, answering machines, video or audio devices.

Employees must

* Use any private offices, rooms or spaces or
* Otherwise take due care to ensure they are not overheard by anyone who has no need to access the information being discussed. For example, calls must not be made or taken in confined public spaces or on public transport.

**10.4 Procedure:**

ADS will spell out its commitment to ensuring that in principle Data Subjects are aware that their data is being processed and

* for what purpose it is being processed
* what types of disclosure are likely, and
* how to exercise their rights in relation to the data

Note that there is no obligation to inform people of anything that is obvious from the context or from general knowledge, or to inform people whose data is obtained from a third party where the cost of informing them would be disproportionate to the risks of holding and using the data: a typical example might be business contact lists.

11. 0 Security

11.1 Security must not be confused with confidentiality. The latter is about defining what is allowed — setting the boundary; the former is about ensuring that the boundary is maintained. However, there must be a relationship between the two.

* Many of the ADS projects are worked on at home. All staff should ensure that any confidential information is secured within a locked cupboard or filing cabinet.
* All passwords should be protected
* There should be back up procedures for all data
* Staff contact details may be given over the telephone but only if this has been allowed by the data subject

**9.0 Responsibilities:**

9.1 All staff are personally liable in their duties for complying with the Data Protection principles.

9.2 Trustees of the charity are responsible for ensuring that they fulfil their duties with regard to the Act.

9.3 All systems which contain information about individuals are identified and made secure. Managers need to be aware of databases holding personal data held by staff and be prepared to justify such databases as required.

9.4 All staff who have access to any kind of personal data should have their responsibilities outlined during their induction procedures.

9.5 A Data Protection policy item will feature on all monthly meetings of the ADS Management team. Any issues will be dealt with in that forum

9.6 Individual meetings can be arranged with the Data Controller to ensure that all the management team are inducted into policy procedures

9.7 It is suggested that when the ADS team contact any business client or contact on behalf of Arts dream organisation that the following is used:

***Save A Tree, Think Before you Print!***

This email and any attachments to it may be confidential or of a privileged nature.  They are intended for the use of the individual to whom it is addressed.  If you are not the intended recipient of this email, you must neither take any action upon its contents, nor copy or show it to anyone, as unauthorised use is strictly prohibited.  Please contact the sender if you believe you have received this email in error and then destroy this and any printed copies in your possession.  Any views or opinions expressed are solely those of the author and do not necessarily represent those of ADS.ADS will not accept liability for any issues arising from viruses, corruption, interception and unauthorised amendment related to this email.

**10. Policy Review**

* The next policy review will be carried out in March 2021
* This will involve the Trustees, The Management team, and selected workshop leaders and representatives of specific projects

**Data audit register 2018**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Category | Data Type | Where from | Type | Where stored | protection | Sensitive  Rating Data | Document retention | Archive or shred | Policy notice needed | Additional  Information | Controller |
| Accounts | Invoices | suppliers | Hardcopy  On line | Accountants  Office.  Treasurer’s office | Locked in steal cupboard in locked office | Low | 7years | Shred | yes | All forms to have private policy retention detail | ADS |
| Accounts | Receipts | Suppliers to know how their details are handled | Hardcopy  On line | Project leader’s office | Suppliers to know how their details are handled | Low | 7years | Shred | yes | Suppliers to know how their details are handled | ADS |
| Individual project  Details | Names  Addresses  Emails  Phone numbers | Project  Participants | Online information  Hard copy | In ADS office  In Project leader’s office | In individual  Project folders, locked in offices | Medium | 7years | Shred | yes | All forms to have private policy retention detail. | ADS |

References:

* The Data Protection Act up date -Gov.uk
* Data Protection Act changes to Legislation ist February 2018
* Charity Commission guidelines for Data Protection January 2018
* Data Protection for local groups Friends of the Earth December 2017
* What your charity needs to know about Data Protection, Market Direct.UK
* HPE Data Protection 2017
* Voluntary Action Chichester Data Protection Guidelines February 2018
* Selsey Community Forum Data Protection form

Chris Butler February 2018, updated June 2019