Updated June 2018

Arts 4 dementia
Empowerment through artistic stimulation

Arts 4 Dementia Policy on Data Privacy and Data Protection

1. Introduction

Privacy risk is the risk of harm arising through use or misuse of personal information. Some of the ways this risk can arise are through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Failure to manage data securely and appropriately may cause harm to staff, donors, clients and other stakeholders, and to the reputation and status of Arts 4 Dementia (A4D)

This policy sets out the principles and processes that A4D should apply to ensure that, in respect of all records that it keeps, as far as reasonably possible it not only complies with the law on data privacy, but also acts in accordance with the wider expectations of our many stakeholders.

2 Applicability

2.1 A4Ds policy on data protection and privacy applies to trustees, staff, contractors, volunteers and others who handle and store Personal Data on behalf of A4D.

2.2 *Data Controller*
A person or legal entity who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. For this purpose A4D is the Data Controller. Staff or Trustees handling Personal Data do so on behalf of the charity.

2.3 *Data Processor*
In relation to Personal Data, any person or organisation (other than an employee of the data controller), such as Donorfy, who processes the data on behalf of the data controller.

3 Collecting and processing Personal Data[i]

3.1 *Legitimate purposes*
General Data Protection Regulation (GDPR) requires that organisations process Personal

Data not only fairly, lawfully but also only for legitimate purposes. A4D will only collect Personal Data where it has a legitimate interest, i.e. necessary to carry out its charitable purposes, for fundraising and, in the case of employees, contractors and other stakeholders, to enable it to undertake its day-to-day operations.

3.2 Individuals will be asked to Consent to their Personal Data being held. We will be transparent about how we will use the data, and give individuals appropriate privacy notices when collecting their Personal Data. Where data has been collected in the past, a request to hold the data will be sought from the individual concerned at the time that it is being assembled into a relevant filing system.

3.3 If Consent is withdrawn, which may be at any time, A4D will promptly respond by removing the relevant Personal Data from its records.

3.4 Data records will be reviewed periodically (at least annually) to identify data, including Personal Data, that is no longer required for the purposes set out above. It may be necessary to re-confirm details with the individuals concerned and this can also be used to update Consent.

4 Additional Conditions for processing Sensitive Personal Data

4.1 a) the individual whom the sensitive Personal Data is about has given explicit Consent to the processing; and

b) one or more of the following:

- The processing is necessary to comply with employment law, legal proceedings or for obtaining legal advice, to meet statutory obligations;
- The processing is necessary to protect the vital interests of the individual (in a case where the individual's Consent cannot be given or reasonably obtained), or another person (in a case where the individual's Consent has been unreasonably withheld) or for medical purposes by a health professional who is subject to a duty of confidentiality;
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals;
- In certain situations, such as preventing or detecting crime and protecting the public against malpractice or maladministration, it is permissible to disclose sensitive Personal Data without explicit approval from the individual concerned.

5 Storing Personal Data

5.1 Personal Data will normally be permanently held in an online database (e.g. Donorfy) as this is considered more secure, as well as more useful than on a laptop.

5.2 Where Personal Data is held in spreadsheets or other structured documents on a laptop then the application should be password protected.

5.3 Personal Data held on laptops or in hard-copy should only be held for as long as required and should be deleted or destroyed when that purpose has been served, if necessary after making necessary changes to the master data.

5.4 If Personal Data for which A4D is responsible is transferred to a private computer, the person responsible should apply good practice in relation to the security of that computer (refer to Computer Security in Appendix 1 "Data Security").

5.5 If Personal Data is processed or shared in e-mails, spreadsheets or other documents, care should be taken not to copy these documents wider than necessary for that purpose (refer also to Email Security in Appendix 1).

5.6 A4D will take appropriate action in the event of a breach of data by recording the breach, notifying the Information Commissioner without delay and notifying the individual concerned where there is a high risk to their rights and freedoms.

6. Sharing of Personal Data

6.1 A4D will not collect or hold Personal Data in order to pass it on to third parties for value and will not share personal data with a third party, other than in the specific cases allowed in the legislation and referred to in 5.3 and 5.4, without the explicit agreement of the Trustees.

6.2 A4D will only disclose Personal Data to third parties in circumstances:

- where required by law;
- where it is in the individual's vital interest, i.e. cases of life and death, such as disclosure to medical practitioner in an emergency;
- at the (written) request of the individual concerned, or in accordance with contracts that individual has entered into.

6.3 Where sensitive personal data is shared with staff and contractors (for example where information relating to the mental or physical wellbeing of clients is shared with facilitators and volunteers at workshops), they will be asked to delete or destroy the data once the immediate need has passed and to confirm that they have done so.

6.4 A third party may request Personal Data where it has a legitimate interest. Requests from a third party must always be balanced against the interests of the individual concerned. The CE will make this judgement, and consult the Chairman or other Trustees where necessary.

7. Requests for Copies of Information held

7.1 GDPR gives any individual the right to find out what information an organisation stores about them. All requests should be passed to the Chief Executive and should only be accepted in writing.

7.2 Normally A4D will endeavour to provide a copy of any record containing Personal Data without charge, but a charge of £10 may be made at the Chief Executive's discretion, to be paid in advance, if significant effort is required to assemble the information or to discourage frivolous or vexatious requests.

7.3 A4D will respond to requests for information held within one month.

8. Contracts with data processors and other third party providers

8.1 Realistically A4D is not in a position to dictate contract terms to large service providers, such as those who may act as Data Processor. Nevertheless it is important that we are aware of the terms on which services are provided and the risks that may follow. The Chief Executive should, to their reasonable satisfaction, ensure that the third party provides processes and systems that manage Personal Data for which A4D is responsible in a manner consistent with GDPR.

8.2 Where practicable, contractors should be notified that compliance with GDPR is a requirement of our contractual relationship and failure to comply will be grounds for termination by us for breach of contract.

9. Personal Data relating to Staff and Trustees

9.1 Information collected for recruitment and selection will only be used for that purpose without the explicit approval of the person concerned. It will only be retained so long as there is a clear need for it. DBS (Disclose and Barring Service) procedures will be followed where checks need to be made and A4D will make a record only that a satisfactory/ unsatisfactory check was made, not hold detailed information on file.

9.2 A4D will not collect or retain information that is irrelevant or excessive to the purpose for which it is collected. Information will be deleted and documents destroyed when there is no longer a clear business need for them to be retained.

9.3 Personal information on staff and trustees will always be labelled as confidential, stored securely and handled with respect.

9.4 Staff and Trustee Personal Data will not be disclosed to another organisation without express permission of the individual concerned, unless covered by the statutory exceptions listed in sections 4 and 5 above. Requests for references will only be given with that persons' consent.

9.5 Only the CE will have access to confidential records with the following exceptions:

- the Chairman will normally hold confidential information relating to the CE and to Trustees;
- the Payroll provider and treasurer will have access to payroll information;
- the size of the charity is such that individual's remuneration will be apparent from financial information prepared for the Trustees.

Appendix 1 - Data Security

Computer security

A4D laptops should have installed appropriate computer security including a firewall and virus-checking software that should be scheduled to run on a regular basis.

Each user is responsible for ensuring A4D data is safe and secure. Good practice should be applied whether the data is held on a computer owned by the charity or a personal one, and includes the following:

a) Ensure that the operating system is set up to receive automatic updates.

b) Always download the latest patches or security updates, which should cover vulnerabilities.

c) Do not share passwords with others. Where more than one person requires access to data then they should have their own passwords.

d) If computers are shared, then A4D data should be protected by separate passwords.

e) Consider encryption of any personal information held electronically that could cause damage or distress if it were lost or stolen.

f) Take regular back-ups and keep them in a separate place so that if a computer is lost, information is not also lost.

g) Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).

h) Install and routinely run an anti-virus and anti-spyware tools to monitor and protect your computer from external threats

i) Do not leave laptops exposed and unattended in public places, bearing in mind that even supposedly secure areas, such as A4D's offices may be accessed by people with criminal intent.

Email security

a) Only share Personal Data by e-mail when absolutely necessary.

b) Make sure you use the right address when sending e-mails. Some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.

c) Use "blind carbon copy" (bcc), not carbon copy (cc) when sending e-mails to multiple users unless the addresses are likely to be known to all recipients (e.g. Trustees or Patrons).

d) If using a group email address, ensure that all recipients are appropriate for the information being sent. In particular it is usually inappropriate, and dangerous, to send Personal Data to groups.

e) Do not send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;

f) When looking at incoming emails be aware of the risk of phishing and other malicious e-mails.
   - Never disclose other persons' Personal Data or any account, credit card details or passwords in response to emails that appear to come from your bank or other familiar third parties. If you believe such requests to be genuine, then you should contact the sender separately (not by return of e-mail) to verify that the requests are genuine (NB: many organisations now ask "security questions" about your Personal Data on the phone, but not in emails. Make sure you are satisfied they are genuine before disclosing anything to them).
   - Do not open spam emails, even to unsubscribe or ask for no more mailings. Use a spam filter or an email provider that has this service.

Faxes and Printers

a) Documents sent to remote printers and faxes may be printed unintentionally and be seen and/or removed by the wrong person. Care should be taken when printing documents that the right destination has been chosen. Recipients of electronic documents may also unintentionally disclose the contents to others.

b) If data is sensitive, or if sensitive Personal Data is included, then you should consider whether sending the information in hard-copy format by a courier service is not more appropriate.

c) Only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.

d) If faxing,
   - make sure you double check the fax number or printer you are using;
   - dial from a directory of previously verified numbers;
   - use a cover sheet, letting anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents;
   - if the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine
   - confirm by phone/email that the whole document has been received.

e) To avoid printing unintentionally to a remote public printer, have the desk-top printer as your default.

Document disposal

Documents containing confidential or Personal Data should not be disposed of in general waste bins but should be shredded.