Aurora Foundation for People Abused in Childhood

DATA PROTECTION POLICY

Author	Nick Gauntlett
Job Title	Chief Executive
Date of Draft	24 May 2018

1. INTRODUCTION

1.1 The Data Protection Act of 1998 covers any information about an individual from which that individual can be identified. The Act applies to ALL personal data whether electronic or manual. The Act requires the Aurora Foundation for People Abused in Childhood (Aurora) to handle such information responsibly, hold it securely, and release it judiciously. There are eight principles defined in the Act which govern the handling of information (see Section 3) and Aurora adheres to these principles.

1.2 Aurora retains relevant personal details of people who have been abused in childhood, therapists involved with service delivery at Aurora, donors, supporters, Trustees and volunteers. Aurora also, as a charitable body, retains information pertaining to the financial management of the organisation that will also be under the jurisdiction of this policy.

1.3 The information is held by Aurora for the purpose of providing a confidential counselling and support to those suffering from mental health distress caused by the impact of childhood abuse in order for them to access the services they need, and for representing their interests. Some data is shared with partner agencies with whom Aurora works (e.g. GPs, other psychological therapy and/or mental health services). Aurora will always inform all individuals that some data is being shared, and with whom.

1.4 The purpose of this document is to set out the commitment of Aurora in how personal information is collected, protected and used. It defines the structure and measures in place to protect data about individuals where necessary.

2. DEFINITIONS

2.1 Data: includes computerised and hard copy filing systems that are structured by reference to individuals and readily accessible; for example counselling notes, outcome forms, client file records, application forms

2.2 Data Controller: is Aurora in its capacity as a collector of information. Any person who handles Personal Data information on behalf of Aurora is bound by the legal requirements of the Data Protection Act. Any such person does not act as an individual but as a representative of the data controller.

2.3 Data Subject: is an individual about whom data is held. Data subjects at Aurora may include:

Users of the Aurora Service (Clients)
Therapists
Volunteers
Trustees
Contact details of people in other organisations
Donors
Supporters

2.4 Personal Data: means data about a living individual who can be identified either (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Examples of electronic personal data include email addresses, videotape, audiotape, CCTV, CDs, contact details, and computerised records that may be processed in documents, emails and databases. Examples of paper-based personal data may be photographs, client files, application forms etc.

2.5 Processing: means virtually everything from data collection, storage and use to data destruction. There is probably nothing that can be done to personal data that would be outside the scope of this Act.

2.6 Sensitive Data: means personal data that includes information about:

- The racial or ethnic origin of the person
- Their religious beliefs or other beliefs of a similar nature
- Their physical or mental health or condition
- Their sexuality
- Their political opinions
- Whether they are a member of a trade union
- Criminal record.

2.7 Financial Data: means any data pertaining to monies generated by the work of the charity through donation or fundraising, including payments made by credit card and bank transfer.

3. THE EIGHT PRINCIPLES OF GOOD PRACTICE TO WHICH AURORA ADHERES

***Lawfulness, fairness and transparency* -** personal data shall be processed fairly and lawfully and, if it is sensitive data, with the explicit permission of the data subject. It is fairly and lawfully processed if:

- Aurora is identified as the Data Controller or processor of any information gathered
- Consent is obtained to collect and process personal information (see Section 4).
- For sensitive data, explicit consent is obtained where possible. This may not be possible where there is confidential counselling, advice or support (see Section 4).
- It is also accepted that data of this nature may sometimes be used for monitoring purposes and in such circumstances safeguards will be in place to ensure that individuals cannot be identified.
- The purposes for which the data obtained may be used, as in Principle 2, are explained to the data subject
- Assurance is given that information obtained will not be used for any other purpose than as specified.

Purpose limitation - 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. Information obtained shall be used for the following purposes:

- Mailing lists, including emailing list for use in contacting individuals. Where consent has been given, this may also be for direct marketing by Aurora. Sometimes shared, visible mailing lists will be used (i.e. for internal emails to Aurora team members, volunteers, Trustees and other internal groups) and permission will be sought from these email recipients. Conversely, a "bcc" (blind carbon copy) format will be used in all external mailings, including those to Aurora clients, to preserve the identities of email recipients.
- Counselling, support and help to adults abused in childhood
- Collating statistical data, which may be published, but will in no way cause an individual's personal information to be disclosed except with their consent
- Any other purpose which specifically promotes the aims and objectives of Aurora whilst conforming to the requirements of the Act. Details of the processing of information falling under the Act will be made publicly available on request.

Data minimisation - personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed. The criteria for collection of information is that it is helpful and useful to the clients for which Aurora exists or that it is relevant to Aurora's operations.

Accuracy - personal data shall be accurate and, where necessary, kept up to date. Information should always be recorded as accurately as possible and kept up to date whenever new information becomes available. The limited uses to which personal data is put means that out-of-date information should not be prejudicial to a data subject, although it might make the service offered less effective. Where data is processed for statistical purposes, efforts are made to ensure that findings are not biased by factors such as outdated information.

Storage limitation - personal data shall not be kept longer than is necessary for the purpose(s) under which the data was collected in the first place.

Contacts & Donors: Kept on file for as long as the relationship with Aurora lasts.
Volunteers & Trustees: Records are kept for various lengths of time to comply with legal requirements.
Clients: For the entire duration of their contact with services rendered by Aurora and archived thereafter in accordance with insurers stipulation, and statutory requirements
Therapists: For seven years after the termination of self-employment, and some data for longer to comply with regulatory requirements.

Integrity and confidentiality - personal data shall be processed in accordance with the rights of data subjects. Personal data is only used for the purposes outlined under Principle 2. Permission to use data for these purposes is requested from the data subject at the time the information is obtained (see also Principle 1). A copy of the information retained will be made available to the data subject on request.

The Act gives rights to individuals in respect of personal data held by others.

The rights are:

- Right to see the data held about them (subject access).
- Right to prevent processing likely to cause damage or distress.
- Right to prevent processing for the purposes of direct marketing.
- Rights in relation to automated decision-taking.
- Right to take action for compensation (see Compensation below) if the individual suffers damage by any contravention of the Act by the data controller.
- Right to take action to rectify, block, erase or destroy inaccurate data.
- Right to make a request to the Information Commissioner (the government body in charge of data protection) in order for an assessment to be made as to whether any provision of the Act has been contravened.

Compensation

Under the 1984 Act data subjects were only allowed to claim compensation through the courts where they had suffered damage as a result of inaccuracy or unauthorised disclosure. This right has been considerably extended to allow the data subject the right to claim compensation for damage caused by any breach of the Act and also for distress in certain circumstances.

Integrity and confidentiality - measures shall be taken to guard against unauthorised or unlawful processing**.** Personal data, whether held on computer or in physical paper files, should be kept secure at all times. Where accidental disclosure occurs, the responsible team member should take swift action to minimise damage. This includes finding out who knows, talking to them and reminding them of their duty to maintain confidentiality, and reporting to Aurora's CEO.

***Accountability* -** personal data shall not be transferred between countries without adequate protection. Computers in Aurora are not connected with others outside the office. The Aurora website does not, and will not, contain any information falling under the Data Protection Act. (Incoming information from the website may contain personal data relating to requests Aurora's services or to be added to one of our mailing lists)[1].

[1] See our Privacy Policy on the Aurora website for more details: www.aurorafoundation.org.uk/privacy-policy

4. CONSENT

4.1 It is not strictly necessary to gain the consent of service users before processing information about them, whether the data is Personal Data or Sensitive Personal Data.

4.2 Consent is not necessary for Personal Data where it is our legitimate interests to hold the information, and holding it doesn't harm the data subject.

4.3 There are some circumstances when consent is needed to use personal data. For 'sensitive personal data' consent may be required. In other circumstances it is good practice to get consent whenever possible

4.4 In the case of Sensitive Personal Data there is an exemption from the need for 'explicit consent' in Statutory Instrument (SI) 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000. This exemption covers cases of confidential counselling, advice or support and getting consent is either impossible or unreasonable (www.hmso.gov.uk/stat.htm has all the Statutory Instruments).

4.5 Consent means informing the person what the information is needed for and asking whether they mind if it is kept. It is possible that someone may later deny that they gave consent, so if this is a possibility a record of the conversation can be sent on initial contact with a new service user. However, written consent is not actually a requirement of the Act but it is good practice to obtain one.

4.6 What constitutes consent? 'Any freely given specific and informed indication of his/her wishes by the data subject signifies their agreement to personal data relating to him being processed'. It cannot be inferred from non-response to a communication.

4.7 As described above there is an exemption from the need for consent in recording sensitive data in the case of confidential support services. Consent from the cared for person or carer of the service user is not needed provided the only recorded information is in order to be able to help the carer or the service user.

4.8 ***Disclosure***

Disclosure of personal information outside Aurora will only be made with the informed consent of the individual concerned, except:

- To comply with the law (e.g. suspected or actual child abuse, acts of terrorism, drug trafficking)
- To comply with a court order
- Where there is a clear health or safety risk to the individual, Aurora team members or a third party
- Where there is evidence of fraud against Aurora

5. STORAGE OF DATA

5.1 ***Computer Data:***

- **Computer security -**Each Aurora Team member has access to an Aurora computer, which can only be accessed by a username and password. The password is never shared and is kept confidential. All electronic files (i.e. word, excel) are encrypted using password protection

- **Memory Sticks -** The use of memory sticks by the Aurora Team to save work related documents are kept to a minimum, and if there is a possibility that they leave the premises they must always be encrypted, so that even if the stick is lost no data breach occurs.

- **Portable Devices (e.g. laptops, tablets and mobile phones) -** Some of the Aurora Team use laptop computers, tablets and mobiles phones but they do not contain personal information and so data security is not compromised.

- **Personal devices -** No Aurora data should be stored on an Aurora Team member's own equipment, be it a computer, mobile phone, memory stick etc. Aurora data can be accessed from a personal device using the internet, for example via the internal wi-fi network, but it must not be held on a personal device.

5.2 ***Manual Data***

- Counselling notes are kept in filing cabinets in the office in the main Aurora building. All cabinets are under lock and key. This information is only accessible to Aurora therapists. Identifying personal data on clients, therapists, volunteers and Trustees is kept in a locked filing cabinet in an office in a separate building. This information is only accessible to Aurora's CEO.

- When papers containing personal details are taken outside the office, they will be transported in a paper self-addressed envelope, so that if they are lost the most likely outcome is that they are posted back to Aurora.

6. DATA BREACHES

6.1 A personal data breach means a breach of security or other incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

6.2 If anyone at Aurora is aware of a personal data breach, they must inform the CEO within 24 hours (or as soon as possible after this) of that breach being identified.

6.3 Details of the breach will be shared with the Chair of TTrustees of the pension schemes and the Trustees will deal with the breach in accordance with their Data Protection Policies.

7. How Long We Keep Your Data

Your data will not be kept for longer than necessary in relation to the purposes for which it was originally collected. We will keep your data for the periods set out below. These time periods, along with our data protection policy, are reviewed regularly and updated if necessary.
We will keep personal information for the following periods:

Data	Retention Period	Reason
Those who have accessed Aurora's support services	For 7 years from the last time you used the service	We need to make sure that we can provide a safe service – this means keeping information so that we can respond to risk. You may want information on your support at Aurora for future services you engage with or if you report to the police. We also need to be able to respond to any complaints made against us.
Donations you've made to us	For 7 years since the date of your last donation	As a charity, we need to keep robust financial records.
Purchasing services, like training or venue hire	For 3 years	As a charity, we need to keep robust financial records.
Subscribing to a newsletter	You can unsubscribe at any time	We will delete your contact details if you no longer want us to contact you.
Information on self-employed therapists	For 6 years after you stop working for us	By law we need to keep certain financial information. We also need to be able to respond to complaints made against us.
Information on vacancy applicants	For 1 year after the job closes	We need to show we have fair application processes and may wish to contact you regarding other jobs.
Information on volunteers	For 6 years after you stop volunteering for us	We need to be able to respond to complaints made against us.

8. Who has access to your data

All information provided voluntarily is used exclusively by Aurora; we do not sell, trade or transfer our data to any third parties unless express consent is given and we do not sell any information about your web browsing activity. The personal information we collect about you will mainly be used by our staff and volunteers so that they can best support you.

We may however share your information with our trusted partners and suppliers who work with us to deliver our services, but we will always make sure that they store the data securely, delete it when they no longer need it and never use it for any other purposes.

9. YOUR RIGHTS

9.1 You have a right to access and control your information and ask us to stop processing your personal data. We will respond to requests for information and, where applicable, will correct, amend, or delete your personal information.

9.2 If you wish to exercise any of these rights or make a complaint, you can do so by contacting our CEO at the Aurora Foundation for People Abused in Childhood, 4 Ebor Cottages, Kingston Vale, London, SW15 3RT, by email at info@aurorafoundation.org.uk or by phone at 0208 541 1951.

9.3 In order to correct, amend or delete any of your personal information, we will need to carry out checks to make sure you are who you say you are.

9.4 It is sometimes not possible for us to delete all of the information we have on you. If you ask for us to delete your data we will let you know if it has not been possible to delete everything we hold on you.

9.5 Alternatively you can make a complaint to the data protection supervisory authority, the Information Commissioner's Office, at ico.org.uk

10. FINANCIAL DATA

10.1 Financial data is anything to do with the management of the charity's finances and income. This is part of general accounting necessary to safe guard the financial stability of the organisation.

10.2 Personal bank details, credit card and other payment information must be held securely and used only for the purposes given e.g. to make payments for services or for setting up salary or expense payments.

10.3 All data will be handled and maintained following Aurora's Financial Controls and the auditing requirements as determined by the Charity Commission and Companies House.