

# ALQUD

## **DATA MANAGEMENT POLICY**

Approved and adopted by Board May 2018

Reviewed April 2021

For review April 2022

### **Context and overview:**

The Aloud Charity needs to gather and use certain information about individuals. These can include members of choirs, funders, suppliers, business contacts, employees, freelance staff, volunteers and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

### **Why this policy exists:**

This data management policy ensures that Aloud:

- Complies with data protection law and follows good practice
- Protects the rights of members, supporters, staff and other partners and stakeholders
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

### **Data protection law:**

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes);
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

**Who? People and responsibilities:**

Everyone at Aloud contributes to compliance with GDPR. Responsibilities include (but are not necessarily limited to):

- Keeping senior management and board updated about data protection issues, risks and responsibilities (Chief Executive)
- Documenting, maintaining and developing the organisation's data protection policy and related procedures, in line with agreed schedule (Chief Executive)
- Embedding ongoing privacy measures into corporate policies and day-to-day activities throughout the organisation. The policies themselves will stand as proof of compliance. (Chief Executive; Development Officer; Project Managers)
- Dissemination of policy across the organisation, and arranging training and advice for staff (Chief Executive)
- Dealing with subject access requests, deletion requests and queries from clients, stakeholders and data subjects about data protection related matters (Administrator)
- Checking and approving contracts or agreements with third parties that may handle the company's sensitive data (Development Officer)
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards (Chief Executive)
- Performing regular checks and scans to ensure security hardware and software is functioning properly (Chief Executive)
- Evaluating any third-party services the company is considering using to store or process data, to ensure their compliance with obligations under the regulations (Chief Executive)
- Developing privacy notices to reflect the lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the companies use of their data (Chief Executive, Development Officer, Project Managers)
- Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles (Development Officer)

**Data Protection Officer (DPO):**

Aloud is not obliged under GDPR to appoint a DPO but has determined that the Chief Executive should fulfil the role of DPO, and lead on ensuring that data protection obligations are met.

The minimum tasks of the DPO are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)

**Scope of personal information to be processed: uses and conditions for processing:**

See the attached spreadsheet (which forms part of this policy) for details of the following:

- What data is kept
- What it is used for
- How it is collected
- Where it is kept
- How long it is kept for
- What the lawful basis for processing is

**Data Sharing and Automated Processing:**

The Aloud Charity does not share data with any other organisation or party. Nor does the Aloud Charity undertake automated processing.

**Security Measures:**

Aloud stores all personal data on a fully GDPR compliant CRM System (eTapestry, a service provided by Blackbaud). Secure log-ons to the system are provided to members of staff who need to access data for the fulfilment of their employment contracts with Aloud. Examples are:

- Administrator and project managers for contacting project participants and parents
- Development Officer for contacting donors, and other supporters
- Finance Administrator for contacting staff and freelance contractors

Hard copies of membership forms for OBA and OKA are kept in a locked filing cabinet within the Aloud office, which is locked outside of office hours, or when there is no-one present.

Lists of data created for specific events (such as Chaperone lists or invite lists) are kept in cloud-based storage, GDPR compliant, and accessible only via password. Laptops, mobile phones and PCs are also password protected, with passwords regularly changed. All equipment is protected with security software and firewalls.

Any hard copies of lists produced for events are kept in folders and destroyed securely after use. This also applies to hard copies of membership forms once obsolete.

**Data Breach**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Certain breaches require reporting to the ICO (Information Commissioner's Office) within 72 hours. A more detailed description of what comprises a data breach is available and is shared with all relevant individuals as part of data protection training. A form for reporting and acting on data breaches is available to all staff, which describes the actions to be taken.

**The Rights of Individuals who are the subject of data:*****Subject Access Requests:***

All individuals who are the subject of data held by the Aloud Charity are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

A subject access request form is available to all staff members, who have been trained in how to complete the form and deliver the data. An example of the form is attached.

***The right to have data rectified:***

The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing and Aloud will respond to this request within one calendar month. (In certain circumstances Aloud can refuse a request for rectification. This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).)

***The right to be forgotten:***

When requested by a subject Aloud will – in certain circumstances - remove from its database all information and data held about that subject.

This will be done by deleting the relevant records on eTapestry, securely disposing of any paper correspondence or records, and the removal of any other contact information held on computers,

phones or other electronic devices. This process will be undertaken by the Administrator, overseen by the Chief Executive.

The right to for personal data to be removed is identified on privacy statements.

**The right to object:** Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

**Privacy Statements:**

Aloud aims to ensure that individuals are aware that their data is being processed, and that they understand:

- Who is processing their data
- What data is involved
- The lawful grounds for processing that data
- The outcomes of data processing
- How long their data is being held
- What their rights are and how to exercise them.

To these ends the Aloud Charity has a number of privacy statements, setting out how data relating to various groups of individuals is used by the company. These statements are shared at first point of contact with the individual. There is also a more generic Privacy Statement available on the website.

**Ongoing documentation of measures to ensure compliance**

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. Records will be kept in the GDPR Compliance file of training of employees on privacy and data protection matters. We will also keep records of privacy measures implemented, and records of compliance.

Aloud

April 2021