ALDEBURGH JUBILEE HALL

DATA PROTECTION POLICY and GUIDELINES

Revised and Approved May 2022

Key Individuals:
The Trustees, collectively, are formally responsible as the Data Controller. However:

David Mackie is designated as the Trustee Lead for Data Protection.

Terezija Hirs (Hall Manager) is designated the Staff and Volunteer Lead for Data Protection implementation.

Background

The Data Protection Act covers the collection and storage of **personal data**, some of which is considered **sensitive**, which is **processed** and **stored** according to the definition defined within the **Data Protection Act**. The **Data Protection Act** (DPA) contains 8 key principles:

- personal data should be processed fairly and lawfully
- data should be obtained only for one or more specified and lawful purposes
- the data should be adequate, relevant and not excessive
- it should be accurate and where necessary kept up to date
- data should not be kept for longer than necessary
- personal data should be processed in accordance with the individual's rights under the act
- data should be kept secure
- personal data should not be transferred outside the European Economic Areas unless the country offers adequate data protection.

The Trustees are ultimately responsible for determining that data is held and processed by any and all **data processors** securely, in order to protect the privacy of the **data subject**. Trustees may delegate implementation to a data manager but this does not remove their ultimate responsibility for ensuring personal data are handled according to the DPA. Failure to correctly comply correctly with the requirements of the DPA may give rise to prosecution and claims for compensation. These obligations apply from the moment that data is obtained to the moment that it is returned, deleted or otherwise destroyed. Data should not be retained for longer than is necessary for the purpose for which it was obtained.

How does this relate to Aldeburgh Jubilee Hall?

In the case of AJH, the personal data collected, processed and stored may include that for:

- Staff and Trustees
- Audiences and marketing activities
- Friends and fundraising
- Casual and contract staff
- Suppliers
- Volunteers

At AJH the Chairty/Company is formally the **data controller** and staff members (and some Trustees and volunteers) are **data processors**. This means that all staff and Trustees need to ensure that the way they are accessing, using and storing personal data is secure enough to comply with the requirements of the **Data Protection Act**. In some cases, external contractors can also be considered **data processors**.

Thus, all Trustees and staff need to be made aware of the act and its implications for their day-to-day work. The following broad guidelines give an overview of what staff need to consider.

Data Protection – Trustee/Staff Guidelines

The DPA defines personal data as information (electronic or paper-based) which relates to a living individual who can be identified:

- from the data
- from the data *plus* other information which is in the possession of, or is likely to come into the possession of, the data controller

The DPA's definition of data processing is very wide and includes:

- obtaining, recording and holding data;
- performing any operation on the data, including the redaction or destruction of the data.

It's important to note that this covers emails and electronic folders; not just those in your inbox and personal folders, but any that are still held on a server or that it is possible to recover.

1. What do we need to tell people about how we store and use their information?

(a) When personal data is obtained, every effort must be made to ensure that the following information is made available to the data subject:

- the identity of the data controller
- the purpose(s) for which the data are to be processed
- the likely consequences of the processing
- to whom the data are likely to be disclosed
- any other information which may be appropriate in the circumstances

(b) If we intend to use personal data for purposes other than those for which they are collected we should adopt an ‘opt-in’ policy for such use whenever collecting personal data.

(c) Where personal data is obtained from someone other than the data subject, the information must be made available to the data subject at the earliest opportunity.

(d) Data subjects must not be misled or deceived as to the purposes for which you are processing their data, or as to whom you may disclose the data.

(e) Personal data should be kept no longer than necessary.

This will be achieved by a general notice about data protection on our website, referred to in any communications using or requesting personal data.

2. How we ensure data subjects have access to their own personal information?

(a) Data subjects have a statutory right of access to their data, so whatever we commit to paper or to the computer - including personal opinions - may have to be retrieved and disclosed to them if a formal enquiry is made.

(b) Data subjects may request copies of personal data being processed about them by the data controller. These requests are known as 'subject access requests'. In response to a valid request, the individual is entitled to be told in an intelligible form:

- whether personal data about them is being processed and, if so, why
- to whom the data may be disclosed
- the source of the data
- Information which identifies a third party may be withheld unless the third party concerned consents to its disclosure.

(c) To enable this Trustees/staff must organise their work appropriately:

- Documents, including emails, which contain personal data should be kept in an orderly fashion and securely filed on registered electronic or paper files as soon as practicable if they are to be retained;
- Personal data and documents should be erased or destroyed when they are no longer required.
- Random collections of odd papers or old emails should not be kept - they should be properly filed.
- All should be satisfied that, if required, they could retrieve personal data for which they are responsible to answer an enquiry from a data subject.

A list should be kept of all who have access to personal data

All Trustees/Staff and others who may have acquire/access/store personal data must be informed of their and responsibilities and helped to fulfil them

3. How do we respond if we receive a request for personal data (a 'subject access request') from a data subject?

(a) Most information enquiries we receive will be informal. If an informal information request is made, for example by phone or email, they should be referred to the Hall Manager to respond informally by providing information or pointing them to the website where they can find it for themselves.

(b) If a formal request is made, either by a data subject or a third party, it is important that this is passed immediately to the responsible individual (Hall manager) who will, as appropriate discuss with the Chair/Hon Secretary. Any request should be checked under the safe disclosure guidance of the ICO to ensure that the request is valid, that the correct data is supplied in the right format and to the right person within the legal time limit.

The Hall Manager is responsible for addressing such requests in the first instance, seeking Trustee advice as appropriate

4. What do we do if there is an information breach?

(a) If an information breach occurs, it is important that this is escalated immediately so that a containment and recovery plan may be implemented. In the event of a suspected breach the Hall Manager must be informed who immediately will inform the Trustee Data Protection Lead and the Chair of Trustees.

(b) In conjunction with the Board Lead and Chair the Hall Manager will create and be responsible for the implementation of a containment and recovery plan. As part of this, the following will be included:

- Assessing the risks – any risks associated with the breach should be reviewed, as these are likely to affect operational procedures once the breach has been contained. In particular, the plan should consider and assess potential adverse consequences for individuals should be assessed; how serious or substantial these are; and how likely they are to happen.

- Notification of breach – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. The plan should be clear about who needs to be notified and why; it should include notifying the individuals concerned; the ICO and other third parties such as the police and the banks if appropriate.

- Evaluation and response – it is important that the causes of the breach are evaluated and also the effectiveness of our response to it. If necessary, policies and procedures should be updated accordingly.