THE BUTLER TRUST

4/9/23

Data Protection and Confidentiality

Policy and Procedures

2023 Review of policy and compliance

There have been no changes in current legislation relevant to this policy since it was last reviewed, and substantially updated, in 2018, to coincide with the introduction of the General Data Protection Regulations (GDPR).

We are satisfied that we are in full compliance with this policy.

Contents

Sources

1 Data Protection Act 1998 (http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)
2 Website of the Information Commissioner's Office (www.ico.org.uk/
3 Data Protection for Voluntary Organisations (2nd edition), Paul Ticher (Directory of Social Change, 2002)
4 Voluntary but not Amateur – A Guide to the Law for Voluntary Organisations and Community Groups, Ruth Hayes and Jacki Reason (Directory of Social Change, 2009)
5 Examples of other organisations' policies from the NCVO policy bank
6 Human Rights Act 1998 (http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1)

1 Policy statement

This document aims to provide staff of The Butler Trust with a framework for the lawful, secure and confidential processing of personal data in accordance with current legislation including, but not restricted to, the Data Protection Act 1998, the Human Rights Act 1998 and the General Data Protection Regulations (GDPR) 2018. The collection, use and sharing of personal data is also governed by common law rules and a duty of care to the individuals whose information is kept.

This document also covers the processing of other confidential data, such as privileged information about royal visits and internal strategic or financial documents.

2 Responsibilities

The Trust is the data controller under the Data Protection Act 1998 and therefore the Trustees are ultimately responsible for compliance with the Act. The Governance Working Group oversees this area on behalf of the Board of Trustees.

Operational procedures and responses to written requests from data subjects will be co-ordinated by the Operations Manager in liaison with the Director. Staff will be consulted when operational procedures are decided.

It is <u>not</u> the responsibility of the Operations Manager to apply the provisions of the Data Protection Act across the organisation. This is the responsibility of the individual collectors, keepers and users of personal data. Therefore staff are required to be aware of the provisions of the Data Protection Act 1998 and their impact on the work they undertake on behalf of the Trust. Staff also have a responsibility to treat other confidential data appropriately, in line with the Trust's procedures and any duty of confidence imposed.

3 Definitions

<u>Data</u>

Data means electronic and paper records, including emails. It also means any expression of opinion about an individual, information held visually in photographs or video clips and information held as sound recordings.

<u>Personal data</u>

Personal data means information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession. Personal data should always be treated as confidential. [See the addendum for more details on personal data stored by the Trust]

<u>Sensitive data</u> (also called sensitive personal data)

In the definition in the Data Protection Act 1998, sensitive data includes information about: racial or ethnic origin; political opinion; religion or belief; trade union membership; health; sexuality; and criminal allegations/proceedings/convictions.

For the purposes of this document, any personal data relating to the following nine protected characteristics as described in the Equality Act 2010 should also be treated as sensitive personal data (some of these overlap with the categories in the Data Protection Act): age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage or civil partnership, pregnancy or maternity.

Security critical data

This is personal information which could, if it fell in to the wrong hands, put someone's safety at risk. In the case of the Butler Trust that includes home addresses of people working within the justice system, past or present. Particular care should be taken with any such data.

Confidential

Confidential means of limited availability to others and referring to specific people, ideas or documents. Confidential data includes personal data. It also includes any other data provided in circumstances imposing a duty of confidence, for example when the data is marked "Confidential" or when the recipient is informed that restrictions apply to holding, using or sharing the data.

Processing

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Data controller

A data controller is a person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Data subject

The data subject is the living individual who is the subject of the personal information (data).

4 Principles of the Data Protection Act

Under the Data Protection Act, personal data must be

- fairly, lawfully and transparently processed – other than in exceptional circumstances that means with the person's informed consent
- processed for one or more specified purposes and not for other purposes
- adequate, relevant and not excessive in relation to the specified purpose/s
- accurate and up to date
- not kept for longer than is necessary for the specified purpose/s
- processed in line with data subject's rights
- secure
- not transferred to countries outside the European Economic Area without adequate protection (this includes putting information on a website).

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right to access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

5 Obtaining personal data

The Trust collects a variety of personal data including information about staff, Trustees, donors, nominees, commendees and award winners. Staff should follow the guidance below when obtaining personal data. The Operations Manager or Director can provide clarification if this is needed.

If personal data is to be obtained, at least one of the circumstances outlined in the section "Principles of the Data Protection Act" must apply.

Staff and others obtaining personal data should include appropriate data protection or privacy statements to ensure the data subject is sufficiently aware of the situation and, in particular, knows:

- who is obtaining their data
- for what purposes they are going to use it
- to whom (in general) the data might be disclosed
- how to exercise their rights (eg how to contact the Trust about their data).

Staff obtaining data should consider whether specific written consent may be required. Written consent is usually required to hold or use sensitive data. This would apply, for example, when taking photographs from which offenders could be identified.

Staff arranging filming or photography of an event should take appropriate steps to inform those who will be present and to act in accordance with the wishes of anyone who does not want to appear in a visual record. Similar steps should be taken when making sound recordings.

If a third party is used to obtain data on behalf of the Trust, the staff member making the arrangements should ensure that the above procedures are followed. The section "Temporary staff and third parties" also applies.

<u>Security critical data</u>

- Because of the potential threats which could be posed by such data getting in to the wrong hands, the Trust should avoid collecting personal (home) addresses wherever possible, should hold such information only with the permission of the person concerned, and should hold such information in hardcopy only stored in a locked cupboard when not in use.

.

6 Keeping data secure

Under the Data Protection Act, appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.

Staff should be aware that personal or otherwise confidential data may be contained in meeting papers, letters, notebooks, emails and written telephone messages; files or documents created for data storage; and on devices such as mobile phones, laptops, and tablets, which might be used in public places or whilst travelling. Staff and others processing data on behalf of the Trust should keep confidential data secure, wherever it is located. This should include the following measures.

Home addresses

- As noted in the previous section, the Trust should avoid collecting personal (home) addresses wherever possible.
- Where someone does not have a suitable alternative address, home addresses should be held only with the permission of the person concerned, and in hardcopy only stored in a locked cupboard when not in use.
- Home addresses should not be stored electronically.
- Home addresses should not normally be included in an email – and may only be so where necessary, with the approval of the Director, following an assessment of the risk / sensitivity of the information concerned – where a home address has been included in an email the email should be permanently deleted from "sent" items afterwards.
- Where home addresses have been included in a letter, any electronic copy kept of the letter should have the address removed from it before it is stored.
- Home addresses should not be included in mail merges (for example in relation to the Award Ceremony, either for hardcopy letters or emails).

Data on PCs, laptops, mobile devices

- All PCs attached to the Office365 server should be password protected.
- Work laptops should be password protected, and have up-to-date virus and firewall protection.
- The Office365 server password should be changed every three months – the laptop and PC passwords should be reviewed at least annually, and updated as required
- As a general rule, files/documents should not be downloaded from the server and should be worked on directly on the server (both for security and information consistency reasons), except for backup purposes.
- Other files containing personal data should only be downloaded to / stored locally on PCs or laptops, or other electronic media, where necessary, and in such cases should be permanently deleted at the earliest opportunity.
- Selected contact details which are used regularly (eg Chair's email address) may be held separately from the contacts database (eg on a laptop/mobile phone) but should be restricted to email addresses/tel. numbers (and should not include home addresses)
- The database should be checked and "cleaned" of any out of date / inappropriate data at least annually.
- Old / out of date data may be retained electronically where there is a clear operational need to do so, with the agreement of the Director, provided they are held on a removable storage facility which is kept secure and disconnected when not in use.
- On office PCs all Outlook folders should be set to auto-archive, to the relevant PC (not the server), after a maximum of 3 months (so that older data can not be accessed remotely)
- Work laptops should only use Outlook with the director's agreement, and where that is given, auto-archive should be set to off (so that outlook data are not stored on laptops)
- Non-work laptops, smartphones etc, should be used to access files on the server only with the agreement of the director – based on a review of the data protection implications
- All passwords should be stored in a file which is itself password protected – and a copy of that password should be kept, in hardcopy only, in a file stored in a locked cabinet

Data on websites

- All websites administered by the Trust should be firewall and password protected.

- Any forums administered by the site (such as on the Changing Lives Together platform) should include clear warnings against posting any confidential or sensitive information; any such information found online should be deleted immediately.

- Any confidential information posted online (such as nomination forms, posted on the Butler Trust site for use by the awarding panel) should have additional password protection, be hidden from search engines, and be deleted when no longer in use).

Hardcopy files

- Hardcopy files containing sensitive or security critical data should be kept in locked cupboards when not in use – this includes: personnel and payroll files; completed gift aid forms; any home addresses kept in hardcopy only at the request of the data subject; and D&D learners' files.

- Files containing personal data should be checked annually and out of date information / information which is no longer required for the purposes for which it was collected, should be securely destroyed.

Secure destruction of confidential data

When confidential data is no longer needed it should be removed or destroyed as follows:

- Confidential paperwork – such as nomination forms – should be shredded.
- Personal data in electronic files should be permanently deleted (including from "recycle bins") as required (however, note that where someone has requested not to be contacted by the Trust, sufficient information should be kept to enable their wishes to be actioned).
- Hard-drives on hardware that is no longer required should be destroyed/wiped professionally.
- Fax ribbons should be destroyed after use, since the correspondence which has been sent by fax (inc. return of forms giving home addresses) can be clearly read from them.

Transferring or sharing data

Personal data sharing outside the office should take place only with the agreement of the Director and after consideration as to whether it is appropriate / allowed to do so under these policies and procedures, and how the data concerned might be kept secure.

7 Keeping data accurate and up to date

Staff and others processing personal data on behalf of the Trust should take all reasonable steps to keep data accurate and up to date.

Electronic mailings should include information on how the recipient can update their data or opt out from future mailings.

Records should be kept of requests from individuals to remove them from mailing lists, and they should be excluded from mailings which apply.

Data should be kept as long as there is a legal requirement to keep the information or for the time needed to carry out the purpose for which it was collected. After that time data should

be destroyed securely as detailed in the section “Keeping data secure: Secure destruction of confidential data”.

8 Use of data in publicity material and on the website

The Trust uses videos, sound recordings, photographs, names and other information in its publicity material and on its website. The Director should ensure that adequate consent has been obtained to use personal data for these purposes.

[See also guidance on websites under “Keeping data secure”]

9 Temporary staff and Third parties

A staff member managing arrangements for a temporary member of staff or third party to carry out work on behalf of the Trust should that they are aware of the Trust’s policies and procedures in respect of data protection and confidentiality and of the requirement to comply fully with them.

Temporary staff should not be given access to personal or otherwise confidential data unless they are being asked to process it. If temporary staff are asked to process such data, the staff member supervising the work should make it clear that the data is confidential and should explain the restrictions which apply.

If data is transferred between the Trust and a third party, the staff member should follow the steps relevant to this in the section “Keeping data secure”.

10 Trustees and volunteers

Trustees and volunteers have a responsibility to follow good data protection and confidentiality practice with regard to data to which they have access in the course of their work for the Trust.

If Trust staff provide confidential data to Trustees or volunteers, staff should make it clear that the data is confidential and should explain what restrictions apply to its storage or use.

Trustees and volunteers processing confidential data should follow the measures in the section “Keeping data secure”. When data is no longer needed for the specified purpose/s, they should return the data safely to the Trust’s office or arrange for it to be securely destroyed.

11 Data subjects’ rights

<u>Objection to processing</u>

Under the Data Protection Act, the data controller has to respond within 21 days to a written objection to processing a data subject’s personal data.

If a staff member receives an objection to processing, they should forward this to the Operations Manager or Director as soon as possible.

The Operations Manager or Director will investigate the objection and take appropriate action in accordance with the Act.

Preventing unwanted communication

If an individual makes a written request for the Trust to stop using their data to make contact with them, the Trust must comply. Allowance can be made for data which has already been processed for a forthcoming campaign, but Trust staff should comply fully with the request within two months at the latest.

Staff should not delete the data subject's details; they should exclude the data from direct marketing by suppression. Suppression involves retaining just enough information about the data subject to ensure that their preferences are respected in future.

Staff should also comply with the measures outlined in other sections of this document for keeping data accurate and up to date across different data sets. This includes recording requests to be excluded from non-essential mailings, communicating these to other staff and applying the information when mailings are sent.

Subject access requests

Individuals have a right to access their personal data, commonly known as the right of subject access. An individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data;
- given details of the source of the data (where this is available).

If a staff member receives a subject access request, they should forward this to the Operations Manager as soon as possible.

The Operations Manager will co-ordinate the response to the request. The response will be made as promptly as possible, and within one month from receipt of the request.

All staff should co-operate by providing the Operations Manager with copies of relevant data which they hold on paper or electronically (including emails). A staff member managing a third party processing data on behalf of the Trust should obtain relevant data from the third party, if applicable.

The GDPR states that you can refuse or charge for requests that are manifestly unfounded or excessive. The Director will decide whether a request should be refused or charged. If a request is refused, you must tell the individual why and that they have the right to complain to the supervisory authority and to judicial remedy. You must do this without undue delay and at the latest, within one month.

The quarterly Director's Report, presented to Trustees at each Trustees' meeting, should include a note of any subject access requests which the Trust receives.

Rights of staff, Trustees, volunteers and contractors

Staff, Trustees, volunteers and contractors are themselves data subjects in respect of the information the Trust processes for the purposes of employment, making contact, managing work and other arrangements. They have the same rights as other data subjects and can expect the Trust to take the same care with their data.

12 Notification with the Information Commissioner's Office

Every organisation which processes personal information must notify the Information Commissioner's Office (ICO), unless there is exemption. Exemption is given to registered charities whose activities fall within areas specified by the ICO.

The Operations Manager will be responsible for checking that the Trust has exemption from the requirement to notify, and will repeat the check whenever there is a change in activity. If there is a requirement to notify, the Operations Manager will arrange the notification.

13 Implementation review

Compliance with this policy should be reviewed annually – at the same time as the policy itself is reviewed (as set out below).

14 Policy review

This policy will be reviewed annually or when there are changes to relevant legislation or the activities of the Trust.

Michael Spurr
Chair

Simon Shepherd
Director

September 2023
To be reviewed September 2024

Addendum

PERSONAL INFORMATION

Contact details etc

We hold / need personally identifiable contact details on a range of individuals, including:

- Award Winners / Commendees
- Trustees and Patrons
- Awarding Panel
- Staff
- Ceremony helpers
- Butler family and other miscellaneous individual ceremony invitees / attendees
- Individual funders
- Palace contacts
- Key stakeholders not covered above

There are a range of different places where contact details might be held electronically, including:

- Main database
- Stored mail merges
- Outlook contacts [on PCs, laptops and phones]
- Outlook sent and deleted items [on PCs, laptops and phones]

Hardcopy files

We keep various hardcopy files which include personal data, including (but not necessarily limited to):

- Learners' files from the D&D programme
- HR files
- Personal contact details (held in hardcopy at request of those concerned)
- Completed gift aid forms