Data Protection Policy

This is a Prince’s Trust staff policy. This policy applies to all employees, volunteers and those working for the Trust on Trust premises, for example, agency staff and staff on secondment from other organisations.

<table>
<thead>
<tr>
<th>Owner</th>
<th>Glen Hymers Senior Head of Security &amp; Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date approved by SMT</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Summary of Changes from Previous Version

⇒ N/A

Title: Data Protection Policy          Doc No: GDPR DOC 1.0
Owner: Security & Risk Management      Author: Glen Hymers
Creation date: April 2018    Last review: May 2018    Next review: April 2019

Once printed this document is no longer controlled
Contents

1. Purpose ......................................................................................................................... 3
2. Scope ............................................................................................................................... 3
3. Policy statement ............................................................................................................. 3
4. Responsibilities and roles under the General Data Protection Regulation ...... 3
5. Data Protection Principles ............................................................................................ 4
   5.1 Personal data must be processed lawfully, fairly and transparently ................. 4
   5.2 Personal data can only be collected for specific, explicit and legitimate purposes ...... 4
   5.3 Personal data must be adequate, relevant and limited to what is necessary for processing .................................................................................................................. 4
   5.4 Personal data must be accurate and up to date with every effort to erase or rectify without delay .................................................................................................................. 5
   5.5 Personal data must be kept in a form such that the data subject can be identified only as long is necessary for processing .................................................................................. 5
   5.6 Personal data must be processed in a manner that ensures the appropriate security . 5
   5.7 The controller must be able to demonstrate compliance with the GDPR’s other principles (accountability) ........................................................................................................... 6
6. Data Subjects’ Rights ....................................................................................................... 6
7. Consent ............................................................................................................................ 6
8. Security of data ................................................................................................................. 7
9. Disclosure of Data ............................................................................................................ 7
10. Retention and Disposal of Data ...................................................................................... 7
11. Data Transfers ................................................................................................................ 8
12. Information Asset Register/Data Inventory .................................................................... 8
13. Document Owner and Approval ..................................................................................... 9
1. **Purpose**

1.1 In order to operate The Prince’s Trust needs to collect certain types of personal information about the people with whom it deals, such as current and past young people, employees, and those with whom it communicates in order to raise funds. This information has to be collected for administrative purposes (such as staff recruitment and the administration of programmes) and to fulfill legal obligations to funding bodies and the government.

1.2 The General Data Protection Regulation (GDPR) requires that as a Data Controller that we are protecting the “rights and freedoms of natural persons” and to ensure that personal data is not processed without their knowledge. The Trust is committed to protecting the rights and privacy of individuals in accordance with the requirements of the GDPR and this document outlines The Prince’s Trust's policy in relation to the Data Protection.

2. **Scope**

1.1 The Prince’s Trust’s Data Protection Policy applies to all staff, secondee’s, contractors and volunteers of the Trust.

1.2 This policy applies to all personal data processing functions, including those performed on young people, employees’, delivery partners’, suppliers’ and volunteers’, and any other personal data the Trust processes from any source regardless of format.

1.3 Outside agencies and individuals who work with the Trust, and who have access to personal information for which the Trust is responsible, will be expected to comply with this policy and with the GDPR and UK Data Protection Legislation.

1.4 Any breach of the policy may result in the Trust, as the registered Data Controller, being liable in law for the consequences of the breach, legal liability may also extend to the individual processing the data and his/her Head of Department or line manager under certain circumstances, in which case the matter. In addition, breach of this Data Protection Policy by staff, secondee’s, contractors or volunteers will be considered to be a disciplinary matter and will be dealt with according to the Trust’s disciplinary procedures.

3. **Policy statement**

3.1 The Prince’s Trust are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information that The Prince’s Trust collects and processes in accordance with the GDPR.

3.2 Any breach of the policy may result in the Trust, as a registered Data Controller, being liable in law for the consequences of the breach, under certain circumstances legal liability may also extend to the individual processing the data and his/her Head of Department or line manager, in which case the matter will be reported to the correct authority. In addition, breach of this Data Protection Policy by staff, secondee’s, contractors or volunteers will be considered to be a disciplinary matter and will be dealt with according to the Trust’s disciplinary procedures.

4. **Responsibilities and roles under the General Data Protection Regulation**

4.1 The Prince’s Trust is a data controller under the GDPR.

4.2 The Senior Management Team (SMT) and all those in managerial or supervisory roles are responsible for developing and encouraging good information practices within their areas of responsibility (AOR).
4.3 The Data Protection Officer, a role specified within the GDPR should be a member of senior management, and is accountable to the SMT for the management of personal data within the Trust, and for ensuring that compliance with data protection legislation and good practice can be demonstrated. The DPO has specific responsibilities in respect to data protection within the Trust and is the first point of call for staff and volunteers seeking clarification on any aspect of data protection compliance. The responsibilities of the DPO can be found within the Data Protection Officer Terms of Reference (TOR).

4.4 Compliance with data protection legislation is the responsibility for all staff and volunteers of The Prince’s Trust.

4.5 The Prince’s Trust Data Protection Training Policy sets out specific training and awareness requirements in relation to specific roles and staff and volunteers of the Trust generally.

4.6 Staff and volunteers of the Trust are responsible for ensuring that any personal data about them and supplied by them to The Prince’s Trust is accurate and up-to-date.

5. **Data Protection Principles**

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The Prince’s Trust’s policies and procedures are designed to ensure compliance with the principles which are described below:

5.1 **Personal data must be processed lawfully, fairly and transparently**

5.1.1 We must identify a lawful basis for processing the data before we can commence processing the personal data e.g. Consent, Contractual, Legal Obligation, Protect the Vital Interests of the data subject, in the public interest or exercise of official authority vested in us as controller or the processing is for the purposes of the legitimate interest pursued by us as the controller.

5.1.2 In order for the processing to be fair, we have to make certain information available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources.

5.1.3 GDPR includes rules on giving privacy information to data subjects\(^1\), these are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. The specific information that we must provide to the data subject can be found in The Prince’s Trust Privacy Notice Procedure which outlines how we aim to achieve this by listing what we will include in our privacy notices. Our standard Privacy Notice is recorded here.

5.2 **Personal data can only be collected for specific, explicit and legitimate purposes**

5.2.1 Data obtained for specific purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of The Prince’s Trust’s GDPR register of processing. The Prince’s Trust Privacy Procedure sets out the relevant procedures.

5.3 **Personal data must be adequate, relevant and limited to what is necessary for processing**

5.3.1 The Data Protection Officer is responsible for ensuring that the Trust does not collect information that is not strictly necessary for the purpose for which it was collected.

\(^1\) Articles 12, 13 and 14
5.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.

5.3.3 The Data Protection Officer will ensure that, on an annual basis all collection methods are reviewed by both internal and external audit to ensure that collected data continues to be adequate, relevant and not excessive.

5.4 **Personal data must be accurate and up to date with every effort to erase or rectify without delay**

5.4.1 Data that is stored by the Prince’s Trust must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume it is accurate.

5.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

5.4.3 It is also the responsibility for the data subject to ensure that data held by the Trust is accurate and up-to-date. Completion of a registration or application form by a data subject will include a statement that the data contained within the form is accurate at the date of submission.

5.4.4 Staff, volunteers and delivery partners are required to notify the Trust of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of the Trust to ensure that any notification regarding change of circumstances is recorded and acted upon, a change of circumstances form can be found here.

5.5 **Personal data must be kept in a form such that the data subject can be identified only as long is necessary for processing**

5.5.1 Where personal data is retained beyond the processing date, it will be pseudonymised in order to protect the identity of the data subject in the event of a data breach. More information on this process can be found here.

5.5.2 All personal data will be kept in accordance with the Retention of Records Procedure and once its retention has passed, it must be securely destroyed as set out in that procedure.

5.5.3 Any requirements for retention passed the specified retention period must be approved by the Information Asset Owner (IAO) within the area of the organisation requesting the retention after consulting the DPO. The justification must be clearly identified and in line with the requirements of the data protection legislation. This approval must be in writing.

5.6 **Personal data must be processed in a manner that ensures the appropriate security**

5.6.1 The DPO will carry out a risk assessment taking into account all the circumstances of the Trust’s controlling or processing operations. In determining appropriateness the DPO will also consider the extent of possible damage or loss that might be caused to individuals (staff or young people) if a security breach occurs, the effect of any security breach on the Trust itself, and any likely reputational damage including the possible loss of customer trust.

5.6.2 When assessing appropriate technical measures, the DPO will consider\(^2\) the following:

a. Password protection,

b. Automatic locking of idle terminals,

\(^2\) Taking into account the requirements of Art 25 and 32 of the GDPR
c. Removal of access rights for USB and other memory media,
d. Virus checking software and firewalls,
e. Role-based access rights including those assigned to temporary staff,
f. Encryption of devices that leave Trust premises such as laptops,
g. Security of local and wide area networks,
h. Privacy enhancing technologies such as pseudonymisation and anonymisation,
i. Identifying appropriate international security standards relevant to The Prince’s Trust.

5.6.3 When assessing appropriate organisational measures the DPO will consider the following:

a. The appropriate training levels throughout the Trust,
b. Measures that consider the reliability of employees (such as references etc.),
c. The inclusion of data protection in employment contracts,
d. Identification of disciplinary action measures for data breaches,
e. Monitoring of staff for compliance with relevant security standards,
f. Physical access controls to electronic and paper based records,
g. Adoption of a clear desk policy,
h. Storing of paper based data in lockable cabinets,
i. Adopting clear rules about passwords,
j. Making regular backups of personal data and storing the media off-site,
k. The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

5.6.4 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

5.6.5 The Prince’s Trust’s compliance with this principle is contained within its Information Security Management System (ISMS), which has been developed in line with ISO27001:2013 and the information security policy set out here.

5.7 The controller must be able to demonstrate compliance with the GDPR’s other principles (accountability)

5.7.1 The Prince’s Trust will demonstrate compliance with the data protection principles by implementing data protection policies and procedures, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

6. Data Subjects’ Rights

6.1 Data subjects have rights regarding data processing, and the data that is recorded about them. These rights can be found in the Subject Access Request Procedure, The Prince’s Trust will ensure that data subjects are able to exercise these rights in a transparent manner.

6.2 Data subjects have the right to complain to the Trust related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints are handled can be found within the Complaints Procedure.

7. Consent

7.1 The Prince’s Trust understands consent to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject’s wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject. The data subject can withdraw their consent at any time. Further detail around consent can be found within the Consent Procedure.
8. Security of data

8.1 All Staff & Volunteers are responsible for ensuring that any personal data that The Prince's Trust holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by The Prince's Trust to receive that information and has entered into a confidentiality agreement.

8.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or

stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media.

8.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Staff & Volunteers of The Prince’s Trust. All Staff & Volunteers are required to read and sign as having understood the Acceptable Use Agreement before they are given access to organisational information of any sort.

8.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation by the IAO for your business area. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the Records Retention Policy and either destroyed in accordance with the Personal Data Destruction Policy or archived in accordance with the Records Archiving Policy.

8.5 Processing of personal data away from Prince’s Trust offices presents a potentially greater risk of loss, theft or damage to personal data. Staff requiring to process personal information away from Trust offices must consult the Acceptable Use Agreement to ensure they are aware of their obligations under this agreement.

9. Disclosure of Data

9.1 The Prince’s Trust must ensure that personal data is not disclosed to unauthorised third parties which include family member, friends, government bodies, and in certain circumstances, the Police. All staff and volunteers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not the disclosure of the information is relevant to, and necessary for, the conduct of the Prince’s Trust’s business.

9.2 All requests to provide data to third parties must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer, further guidance on these types of disclosure can be found here.

10. Retention and Disposal of Data

10.1 The Prince’s Trust shall not keep personal data in a form that permits identification of data subjects for a longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected. The retention period of each category of personal data is set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations for which have to retain the data.
10.2 The Prince's Trust may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific to the implementation of appropriate technical and organisational measures to safeguard the rights freedoms of the data subject.

10.3 The Prince’s Trust’s data retention and data disposal procedures will apply in all cases.

10.4 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the “rights and freedoms” of data subjects.

11. Data Transfers

11.1 The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

11.1.1 An adequacy decision: The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

11.1.2 Privacy Shield: The Prince’s Trust will only share data with organisation’s in the United States if they are signatory to the Privacy Shield Framework as administered by the U.S. Department of Commerce

11.1.3 Model Contract Clauses: The Trust may adopt approved model clauses for the transfer of data outside of the EEA, by adopting these model clauses there is an automatic recognition of adequacy.

11.1.4 In the absence of an adequacy decision, Privacy Shield membership, or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject’s request;

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;

e. the transfer is necessary for the establishment, exercise or defence of legal claims; and/or

f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

12. Information Asset Register/Data Inventory

12.1 The Prince’s Trust has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project.

12.2 The Trust is aware of any risks associated with the processing of particular types of personal data. It assesses the level of risk to individuals associated with the processing of their personal data through the use of Data Privacy Impact Assessments (DPIAs) (DPIA Procedure GDPR DOC 2.4 and GDPR REC 4.4) are carried out in relation to the processing of personal data by the Prince’s Trust, and in relation to processing undertaken by other organisations on behalf of the Trust. The Trust will
manage any risks identified by the risk management process in order to reduce the likelihood of a non-conformance with this policy.

12.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of a natural living person, the Trust shall, prior to the processing, carry out a DPIA. A single DPIA may address a set of similar processing operations that present similar high risks. Where as a result of a DPIA it becomes apparent that the Trust is about to commence processing of personal data that could cause damage and/or distress to data subjects, the decision as to whether to commence must be escalated to the Data Protection Officer. The DPO will if there are significant concerns, either as to the potential damage or distress, or the quantity of the data concerned, escalate the matter to the Supervisory Authority.

13. **Document Owner and Approval**

13.1 The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

13.2 A current version of this document is available to all members of staff on The Loop and is published annually in accordance with Prince’s Trust Policy.

13.3 This policy was approved by the Senior Management Team on [date] and is issued on a version controlled basis under the signature of the Chief Executive Officer (CEO).

![Signature](signature.png)

Signature: Date: 25-05-2018

**Change History Record**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description of Change</th>
<th>Approval</th>
<th>Date of Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial issue after draft revisions</td>
<td>Phil Rustage</td>
<td>25-05-2018</td>
</tr>
</tbody>
</table>

PUBLIC