| | | |
|---|---|---|
| | **Data Protection Policy** | |

| | | Last review date | Next review date |
|---|---|---|---|
| Approved by policy committee | | 1st March 2016 | 1st March 2017 |
| Approved by trustees | 6th February 2015 | | |
| Website (yes/no) | Yes | | |

## CQC Fundamental Standards Compliance

The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014**:**
**Regulation 17, Good Governance**
**Regulation 21, Records**

## Relevant Legislation and Guidance:

**Data Protection Act 1998**

**Freedom of Information Act 2000**

## Introduction

Scott's Project Trust (the Trust) is required to process relevant personal data regarding its service users, staff, volunteers and trustees as part of its operation and in order to comply with its legal obligations.

The Trust is committed to compliance with the Data Protection Act 1998 (DPA). Personal data will be collected and used fairly, stored safely and not disclosed unlawfully.

The Trust is registered with the Information Commissioner as a Data Controller, the registration number is Z3063291.

## Aim

The aim of this policy is to ensure that all staff, volunteers and trustees handling personal data are fully aware of and abide by their duties under the DPA.

## Scope

This policy identifies the main principles of the DPA which must be adhered to when processing personal data by or on behalf of the Trust however collected, recorded and used including all manual, electronic and other records.

### Clarification of terms used

1.Throughout this policy reference is made to the 'Senior Manager.'

For clarification, this includes the term 'Registered Manager' which is used for the Senior Managers of the CQC registered services, that is residential care at St Peter's Row, and the Supporting Independence Service which is delivered at the Oaks and Willows. The Development Centre Senior Manager is an unregistered position.

2. Reference is made to 'Manager' which for the purposes of this policy refers to the Office Manager and the Facilities Manager

Each Senior Manager/Manager has the delegated responsibility of Data Protection Officer (DPO) within the service / department which they are responsible for.

3.Reference is also made to 'staff' which for the purposes of this policy refers to everybody who works in a paid or voluntary capacity for or on behalf of the Trust.

## The Data Protection Act 1998 (DPA)

The Trust shall comply with the Data Protection Principles contained within the DPA to insure all personal data is

- Obtained fairly and lawfully and not be processed unless certain conditions are met
- Obtained for a specific and lawful purpose
- Adequate, relevant but not excessive
- Accurate and kept up to date

- Not be held longer than necessary
- Processed in accordance with the rights of data subjects
- Subject to appropriate security measures
- Not transferred outside the European Economic Area (EEA.)

## Policy Implementation

In compliance with the principles of the DPA, all staff will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why personal data is required at the outset:
- Ensure that only the minimum amount of personal data needed is collected and used;
- Ensure the personal data used is up to date and accurate;
- Review the length of time personal data is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised This will include:

    - The right to be informed that the processing is being undertaken
    - The right of access to their personal information
    - The right to prevent processing in certain circumstances
    - The right to correct, rectify, lock or erase incorrect information.

The Trust will ensure that:

- All staff managing and handling personal data are appropriately trained
- Anyone wanting to make enquiries about handling personal data, whether a member of staff, service user or their representative, knows what to do;
- Any disclosure of personal data will be in line with the Trust's procedures.

## Key Operational Framework

Processing of personal data will only be carried out where the member of staff or service user has given consent. This includes implied consent, for example where the personal data is necessary for the performance of a contract to which the individual subjects are a party; or

- for taking steps at the request of a job applicant, service user or their representative, with a view to entering into a contract of employment or other legal obligation such as an offer of care and / or support services;
- the processing is necessary for performing any obligation imposed by law on the Trust in connection with offers of care and /or support services or employment; or
- the processing is necessary in order to protect the vital interests of the individual or another person in a case where (1) consent cannot be given by the individual; (2) The Trust cannot be reasonably expected to obtain the consent or (3) in order to protect the vital interests of another person in a case where the consent by or on behalf of the individual has been unreasonably withheld.

- Details of the reasons why the personal data is sought, and the reasons for which it will be used will be stated on all relevant Trust forms. This is a Data Protection Statement(s). The Trust uses a number of statements which are outlined in Appendix 2.
- The processing of sensitive personal data will only be carried out with the individual's explicit consent as outlined in the Trust's Data Protection Statement(s). See Appendix 2. Sensitive personal data is defined at Appendix 1.
- Data received from third parties – Personal data which has been provided to the Trust, in confidence, by a third party such as employment references cannot normally be disclosed to the data subject, unless the author of the data (third party) can remain anonymous, agrees to the release of the information at a later date or it is reasonable to comply with the access request without the originator's consent.
- Where personal data is held by the Trust on service users, staff and other individuals, these people have the right to access the information, unless it is exempt under the Data Protection Act.
- Where a request for information is received (this must be in writing, including e-mail correspondence), The Trust will respond to the request within 40 days as set out in the Access to Personal Information Procedure. See Appendix 4.

- The Trust is registered with the Information Commissioner. The Registration form is held in the Finance and Administration Department. The Finance and Administration Manager shall ensure all ongoing requirements for registration are complied with and will liaise with the Senior Managers and the Board of Trustees on the content of the registration.

- The Trust has an audit procedure for Senior Managers to undertake periodic reviews of the information being processed within their service / department.

- The following policy and procedure documents have been developed and implemented to endeavour to ensure the Trust's compliance with the principles of the DPA as these apply to the day to day activities of the Trust.

    - Acceptable Internet Use Policy
    - E-mail, Messaging and Social Media Acceptable use Policy
    - Site Security Policies
    - Network Security Policies
    - Laptop and Mobile devices Policy
    - Confidentiality Policy
    - Information Audit Procedures

## Responsibilities for compliance

The Board of Trustees has the overall responsibility for personal data held by the Trust. This responsibility is delegated to the Senior Managers who are the Data Protection Officers (DPO) for the service / department which they manage.

The Senior Managers are responsible for:

- Understanding, upholding and communicating to staff The Trust's obligations under the Act

- Safeguarding the personal and sensitive data held on individuals within their service / department

- Identifying potential problem areas and risks

- Producing clear and effective procedures

- Monitoring and reporting to the Service Management Committee on compliance

The Finance and Administration Manager, with day to day running delegated to the Office manager, is responsible for:

- Notification and registering with the Information Commissioner
- Co-ordinating any amendments to the Trust's registration
- For matters relating to Network security

- Liaison with the Information Commissioner as required, for example where there is a breach of data protection principles
- Ensuring that the storage of digital data, systems back up, storage and disposal of digital media and Network systems are secure

- Ensuring that associated Network Policies and procedures underpin and align with this Policy.

It is the individual responsibility of each member of staff to ensure they comply with the Trust's Data Protection Policy and associated procedures.

Breach of this Policy will be dealt with in line with the Trust's Disciplinary Policy.

## Security of data

- All members of staff are responsible for ensuring that any personal data which they hold in line with the Trusts Policy is kept securely and that it is not disclosed to any unauthorised third party.

- All personal data should be accessible only to those who need to use it.

- Manual records must be stored in a locked drawer or filing cabinet. Computerised data must be stored securely.

- Care should be taken to ensure that PC monitors and Mobile Device Screens are not visible except to authorised staff and that computer passwords are kept confidential.

- PC's, Mobile Phones and Laptops must not be left unattended without password protected screen savers and manual records must not be left where they can be accessed by unauthorised personnel. Staff are encouraged to operate a "clear desk" policy when finishing work each day.

- Care is taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records are shredded or disposed of as "confidential waste". All disposal of Network equipment will be managed by the Finance and Administration Manager and in accordance with the Waste Electrical & Electronic Equipment (WEEE) directives and the Trust's Network Security Policy thus ensuring data destruction and system security.

## Retention & Disposal of data

- The Trust discourages the retention of personal data for any longer than is necessary. Considerable quantities of personal data are collected and some

will be kept for longer periods, however every effort is made to review the need to keep it and safely to dispose of such data as soon as possible. See Appendix 3 -Retention of Records. The Senior Managers regularly review the personal data to be disposed of in accordance with data auditing procedures. The Trust will comply with external guidelines on the retention of records where appropriate. See Appendix 3- Retention of personal data records. Personal data will be disposed in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, deletion from Network systems and backups).

## Monitoring and review

- On a pre-determined basis prior to annual re-registration with the Information Commissioner, the Finance and Administration Manager will provide the Senior Managers with a copy of the Trust's registration requesting that this be reviewed with any proposed amendments incorporated into the registration.

- Any changes to Trust's registration will require the permission of the Board of Trustees before being submitted to the Information Commissioner.

- Any breaches of this policy or associated procedures will be reported to the Board of Trustees annually in summary format together with details of the number of subject access requests and whether or not these access requests have been arranged within the time period set out by the DPA.

## Training

- All new staff will read the Data Protection and Confidentiality policy during their induction.

- Existing care and support staff receive training covering the information held within service user's records.

- The Senior Managers are trained appropriately in order to understand their responsibilities under the Data Protection Act 1998.

**APPENDIX 1**

## DATA PROTECTION DEFINITIONS USED IN THIS POLICY

**Data Controller –** a person or organisation who decides how personal data is to be processed and for what purpose.

**Data Subject –** data subject means an individual (not an organisation), who is the subject of personal data such as a service user or member of staff.

**Data** (including manual data/relevant filing system) – information which:

a) is being processed by means of equipment operating automatically in response to instruction given for that purpose,

b) is recorded with the intention that it should be processed by means of such equipment;

c) is recorded as part (or with the intention that it should form part) of a relevant filing system (i.e. any set of information relating to individuals to the extent that, although not processed as in (a) above, the set is structured, whether by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible); and

d) does not fall within paragraph a), b), or c) but forms part of an accessible record as defined in Section 68 of the DPA.

Examples of manual data that may qualify as structured manual files:

- Personnel Files – applications forms, appraisal forms, disciplinary records, sickness records, supervision notes etc.
- Service user Records – care plans, risk assessments, financial records, medical records etc.

**Personal Data** – all data relating to a living individual who can be identified from that data. This includes any expressions of opinion about that individual as well as any intentions that any person has regarding that individual.

**Sensitive Personal Data –** includes the following and where processed by the Trust the explicit consent of the appropriate individual will generally be required in writing:

- Racial or ethnic origin;
- Political opinions;
- Religious or similar beliefs;
- Trade union membership;
- Mental or physical health;
- Sex life;
- Criminal records or allegations of criminal conduct.

**Processing –** the management of data or information includes obtaining, recording, holding, organising, adapting consulting, retrieving or otherwise performing some operation on it.

Processing also includes disclosure of data and destroying data or information.

Almost all uses of data or information are included in the definition of processing.

**APPENDIX 2**

# THE TRUST'S DATA PROTECTION STATEMENTS

The Trust has the following statements which are added to the Trust's forms or documents as necessary to comply with the DPA.

**Data Protection Statement added to Service User forms or documents**

The Trust is committed to compliance with the Data Protection Act 1998 (DPA.) Personal data will be collected and used fairly, stored safely and not disclosed unlawfully.

**Data Protection Statement added to Recruitment forms or documents**

The data collected on this form will only be used for the purpose of recruitment within the Scott's Project Trust and will not be disclosed to any external sources, except as required by law, without your express written consent. Both electronic and paper records will be stored in accordance with the Data Protection Act 1998.

**Data Protection Statement added to Administration forms or documents**

The data collected on this form will only be used for the purpose of internal administration within the Scott's Project Trust and will not be disclosed to any external sources, except as required by law, without your express written consent. Both electronic and paper records will be stored in accordance with the Data Protection Act 1998.

**Data Protection Statement added to Fundraising forms or documents**

The data collected on this form will only be used for the purposes of informing you about, and fundraising for, the work of Scotts Project Trust. It will not be disclosed to any external sources, except as required by law, without your written consent. Both electronic and paper records will be processed in accordance with the Data Protection Act 1998.

**APPENDIX 3**

## RETENTION OF SENSITIVE PERSONAL DATA RECORDS

The Trust processes personal data on a number of different subjects; these include the service users, the staff, applicants for employment and members of the board of Trustees.

The Trust will endeavour to ensure that all data is processed in accordance with the principles of the Data Protection Act and will be retained securely for as long as it is required.

Sensitive Personal Data will be kept in recognised secure systems with controlled access. All sensitive data processed by the Trust is listed below with retention period and storage criteria. Other information, for example minutes of the Trustee meetings, which falls under Company Law, is omitted from this Appendix.

The Trust will comply with legislation and good practice advice wherever possible to ensure that data is kept only for as long as it is legally required and is securely destroyed thereafter.

| **Data Type** | **Service / Department** | **Retention Period** | **Storage** |
|---|---|---|---|
| Service user files | SPR, S.I.S, DC | 50 Years | Secure locked location |
| Service user Medication Records | SPR, S.I.S, DC | 50 Years | Secure locked location |
| Service user Financial Records | SPR, S.I.S, DC | 50 Years | Secure locked location |
| Employment Files | Finance and Administration | 50 Years | Secure locked location |

# ACCESS TO PERSONAL INFORMATION PROCEDURE

1. Any member of staff, who wishes to receive a copy of any personal data covered by the DPA held electronically or held on a manual file, should submit a written request to their Senior Manager or to another Senior Manager. Where the member of staff is a Senior Manager, the written request should be submitted to a Trustee.

2. Within 40 days of receipt of the written request, arrangements will be made for the file /data to be viewed at a suitable and convenient location. A Senior Manager will be present during the viewing. The file / personal data may not be taken away, or any of its contents removed.

3. No charge will normally be made for requests for information. However the Trust reserves the right to make a charge of up to £10 to contribute towards administration, stationery and postage costs where it is felt necessary to do so.

4. The member of staff may ask for inaccurate or misleading information to be corrected, but no amendments or alterations may be made to the file / personal data by the member of staff.

5. The Senior Manager or Trustee will instruct the Finance and Administration department to make the necessary corrections to the information held.

6. Members of staff are permitted to take photocopies of documents within their file / personal data if they wish. This will be facilitated on the Trust's premises.

The Trust endeavours to keep all personal data up to date and accurate.

- Each year, all staff will be issued with a form showing the main information kept on the staff database. Staff are asked to return these forms with amendments, if required, to the Finance and Administration department.

- Service User personal data is reviewed with the Service User and / or their representative annually at a care / support review.