OP	General Data Protection Regulations (GDPR) Policy	1

		Last review date	Review Frequency	Next review date
Approved by policy committee		12th December 2018	Annually	12th December 2019
Website (yes/no)	Yes			

Introduction

Scotts Project Trust ("The Trust") is committed to conducting its business in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

This policy sets forth the expected behaviours of the Trust's staff and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a service user, a member of staff, external agency staff, a volunteer, a contractor, a donor or a supplier

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. The Trust as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose the Trust to complaints, regulatory action, fines and/or reputational damage.

The Trust is fully committed to ensuring continued and effective implementation of this policy, and expects all of The Trust's staff and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action in line with the Trust's Disciplinary Policy, or business sanction.

Scotts Project Trust is registered with the Information Commissioners Office (ICO). The registration number is Z3063291

2. Scope

This policy applies to all Personal Data processed by The Trust.

The Data Subjects are:

- Service users;
- Staff and Volunteers;
- External Agency Staff;
- Children on community enrichment and work experience placements;
- Donors and Supporters
- Hall and Barn hirers

This policy applies to the Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

3. Definitions

Service User- Any person in receipt of services provided by the Trust

Staff - An individual who works part-time or full-time for the Trust under a contract of employment.

External Agency Staff- An individual who works at Scotts to cover staff shortages, who is employed by an external agency.

Volunteer- An unpaid individual, who gives up their time to support the work of the Trust.

Senior Manager- The Registered Manager of St Peter's Row (SPR), the Registered Manager of the Supporting Independence Service (SIS), the Development Centre (DC) Manager and the Senior Finance and Operations Manager.

CEO- The Chief Executive Officer employed by the Trust.

Independent Contractors - An Independent Individual who works on behalf of the Trust.

Donor- An individual who donates money to the Trust.

Supporter- An individual who is interested in work of the Trust.

Hall and Barn hirers- An Individual who 'hirers' the Trust's Hall or Barn for private use.

Third Party- An external organisation.

Personal Data - Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

Identifiable Natural Person- Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller-The Person or Organisation legally responsible for processing Personal Data i.e. the Trust

Process, Processed, Processing- Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection-The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Processors- A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Consent - Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Special Categories of Data Personal Data- Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Profiling- Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Personal Data Breach- A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Encryption- The process of converting information or data into code, to prevent unauthorised access.

Pseudonymisation- Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Anonymisation Data- amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Governance

The Trust does not have an appointed Data Protection Officer. Sue Bourne is the Trustee with the oversight for Data Protection.

The Trust employs a CEO, who will act as the point of contact for and cooperating with Information Commissioner's Office (ICO)

The CEO will-

- Determine the need for notifications to the ICO as a result of current or intended Personal Data processing activities;
- Make and keep current notifications to the ICO
- Ensure that there is a procedure to provide prompt and appropriate responses to Data Subject requests;
- Inform the Trustee with oversight for Data Protection of any potential corporate, civil and criminal penalties which may be levied against The Trust and/or its Staff for violation of Data Protection law.
- Ensure the establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:
    - provides Personal Data to The Trust,
    - receives Personal Data from The Trust,
    - has access to Personal Data collected or processed by The Trust,

Dissemination & Enforcement

The Senior Managers will ensure that all staff, external agency staff and volunteers responsible for the Processing of Personal Data are aware of and comply with the terms of this policy.

In addition, the Senior Managers will make sure all Third Parties engaged to Process Personal Data on behalf of the Trust are aware of and comply with the terms of this policy.

Assurance of such compliance must be obtained from all Third Parties, prior to granting access to Personal Data controlled by The Trust.

Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems and/or processes, each of them must go through an approval process before continuing.

The Senior Manager must ensure that a Data Protection Impact Assessment (DPIA) is conducted, for all new and/or revised systems or processes for which they have responsibility.

The findings of the DPIA must then be submitted to the CEO for review and approval. Where applicable, the Information Technology (IT) department, will cooperate with the CEO to assess the impact of any new technology uses on the security of Personal Data.

Compliance Monitoring

To confirm that an adequate level of compliance is being achieved in relation to this policy, the Trust will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess:

• Compliance with Policy in relation to the protection of Personal Data, including:

- The assignment of responsibilities.
- Raising awareness.
- Training of Staff and Volunteers.

• The effectiveness of Data Protection related procedures including:

- Data Subject rights.
- Personal Data transfers.
- Personal Data incident management.
- Personal Data complaints handling.
- The level of understanding of Data Protection policies
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.
- The adequacy of procedures for redressing poor compliance

In addition to the annual compliance audit the Senior Managers will carry out quarterly reviews to identify inaccurate records, remove irrelevant records and to update out of date records.

Personal Data Breaches.

The Trust will devise a plan to repair and mitigate any damage or harm caused by accidental or deliberate loss of Personal Data or breaches of the established policies and procedures in the Processing of Data within a defined and reasonable time frame.

Staff who fail in their duty of care to protect Personal Data may be subject to disciplinary proceedings in line with the Trust's Disciplinary Policy.

Data Protection Principles

The Trust has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

• Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

This means The Trust must tell the Data Subject what Processing will occur (transparency) the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

• Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

This means The Trust must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

• Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

This means The Trust must not store any Personal Data beyond what is strictly required.

• Principle 4: Accuracy

Personal Data shall be accurate and, kept up to date.

This means The Trust must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed.

This means The Trust must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

• Principle 6: Integrity & Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The Trust must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

• **Principle 7: Accountability**

The Trust shall be responsible for, and be able to demonstrate compliance.

This means The Trust must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Data Collection

Personal Data should be only collected from the Data Subject unless one of the following apply:

- The Data Subject is a service user who is being placed at St Peters Row (SPR), the Development Centre (DC) or Supporting Independent Living (SIS), and the Personal Data required is in the form of a waiting list form/referral form/needs assessment/ care plan/care matrix.
- The Personal Data relating to a service user is received from a Health or Social Care Professional.
- The Personal Data is received from the Disclosure and Barring Service (DBS) following a DBS check.
- The Personal Data is received from a Referee.
- The Personal Data is received from Occupational Health.
- The Data Subject is an External Agency member of care staff.

When Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection promptly, unless the information must remain confidential.

Data Subject Consent

The Trust will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, The Trust is committed to seeking such Consent.

The Trust shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:

- Determining what disclosures should be made in order to obtain valid Consent.

- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given.
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

Data Subject Notification

The Trust will provide Data Subjects with information as to the purpose of the Processing of their Personal Data

- When the Data Subject is asked to give Consent to the Processing of Personal Data
- When any Personal Data is collected from the Data Subject.

All appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- . The Data Subject already has the information
- . A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing.

Data Processing

The purpose of processing the Personal Data of service users, staff, volunteers, agency staff and contractors, community enrichment and work experience placements, donors and supporters, and Hall and Barn hirers. is listed in each of the Privacy notices. These can be viewed within each department or on the secure server Policy/9.Trustwide forms letters notices/Notices.

The Trust will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of an employment contract.
- Processing is necessary for compliance with CQC Regulations and/or contracts with Local Authorities.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

- Where The Trust has assessed and recorded a Legitimate Interest to process personal data.

In any circumstance where Consent has not been gained for the specific Processing in question, The Trust will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Trust.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

Special Categories of Personal Data Policy

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so
- One of the special conditions for processing sensitive personal information applies:

(a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of The Trust or the data subject
(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
(e) the processing relates to personal data which are manifestly made public by the data subject
(f) the processing is necessary for the establishment, exercise or defence of legal claims
(g) the processing is necessary for reasons of substantial public interest

(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services

(i) the processing is necessary for reasons of public interest in the area of public health.

The Trust's privacy notice(s) set out the types of sensitive personal information that we processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless The Trust can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that The Trust can demonstrate compliance with the GDPR.

Children's Data

The Trust Processes the Personal Data of the Children who attend the Development Centre for community enrichment days and work experience placements. The Data consists of:

- Contact details
- A photograph
- Known allergies and GP contact details

Consent to Process is sought by the Senior Manager, from a responsible adult at the School.

Data Quality

The Trust will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject.

The measures adopted by the Trust to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.

- Restriction, rather than deletion of Personal Data, insofar as:
  - a law prohibits erasure.
  - erasure would impair legitimate interests of the Data Subject.
  - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

Profiling & Automated Decision-Making

The Trust does not engage in Profiling and automated decision-making.

Digital Marketing

As a general rule The Trust will not send promotional material to a Contact through digital channels such as, email and the Internet, without first obtaining their Consent.

Data Retention

To ensure fair Processing, Personal Data will not be retained by The Trust for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

The length of time Personal Data needs to be retained is set out in the 'Personal Data Retention Schedule'. Appendix 1. All Personal Data will be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

The Trust has adopted physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum security measures adopted are to:

- Prevent unauthorised persons from gaining access to the server / manual filing cabinets in which Personal Data is Processed / stored.
- Prevent staff from accessing Personal Data beyond their needs and authorisation.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified or removed from a data processing system.

- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Senior Manager.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is Processed separately.
- Ensure that Personal Data is not kept longer than necessary.

Data Subject Requests

The Trust has a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, The Trust will consider each such request in accordance with the General Data Protection Regulations.

No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Senior Manager, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The retention period for the Personal Data.

Data Subject Requests

The right of the Data subject to:

- Object to Processing of their Personal Data.
- Lodge a complaint with the CEO.
- Request rectification or erasure of their Personal Data.
- Request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Senior Manager, who will log each request as it is received. A response to each request will

be provided within one month of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

Data Subjects have the right to require The Trust to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If The Trust cannot respond fully to the request within one month, it may extend the timeframe by a further two months. The Senior Manager will provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and the procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the CEO.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Where appropriate, Third party Data Processors will be informed of the rectification or erasure of Personal Data.

Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime, for example Adult Protection cases.
- The apprehension or prosecution of offenders.
- By the order of a court or by any rule of law.

Data Transfers

The Trust only transfers Personal Data where one of the transfer scenarios listed below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject for example Payroll.
- The transfer is necessary for the conclusion or performance of a contract with a Third Party in the interest of the Data Subject, for example to a Local Authority.
- The transfer is legally required, for example to CQC.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.
- Where The Trust has assessed and recorded a Legitimate Interest to transfer the personal data, for example to the NMDS –SC data base.

Transfers to Third Parties

The Trust will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, The Trust will first identify if, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, the Trust will enter into, an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, The Trust will enter into, an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data incompliance with The Trust's instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

When The Trust outsources services to a Third Party, it will be identified whether the Third Party will Process Personal Data on its behalf. The Trust will make sure that adequate provisions for such Processing are detailed in the contract.

The Senior Managers shall conduct regular audits of the Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to The CEO.

Complaints Handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Senior Manager An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The

Senior Manager will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and Senior Manager, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the ICO.

Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify their Senior Manager or another Senior Manager in their absence or the CEO providing a description of what occurred. See Appendix 2 for the Data Breach Reporting Policy.

The CEO or authorised person will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the CEO will co-operate with Third Parties involved in the breach, including the Police if there is evidence that criminal acts have been committed.

Where the Trust processes personal data on behalf of a Local Authority/NHS, the CEO will inform the Local Authority/ NHS of the breach, as soon as is reasonably possible, to enable the Local Authority/NHS, as the Controller, to report the data breach to the ICO within 72hours.

The Trust will also take action against Third Parties who have not followed the require policies and procedures.

Where a Data Subject has suffered significant harm from Personal Data breaches or is placed at high risk of being harmed, The CEO will inform the ICO so that it can investigate.

Data Protection Training

All Staff who have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff induction training.

In addition, the Senior Managers will provide regular Data Protection procedural guidance for their staff. Appendix3

Appendix 1

Service User Data Retention Periods

	Document / Record	Department	Storage	Retention Period	NHS funded service users
SPD	Risk Assessments	SPR,SIS,DC	Hard copy /Server	Keep latest Risk assessment until a new one replaces it	
SPD	PEEPS Forms	SPR,SIS,DC	Hard copy/Server	Keep latest PEEP assessment until a new one replaces it	
SPD	Potential Service User Referral/Waiting list Forms	SPR,SIS,DC	Hard copy/ Server	1 year	
SPD	Photographic Images Consent	SPR, SIS,DC	Manual / Server	1 year	
SPD	Mental Capacity Assessments	SPR,SIS,DC	Hard Copy / Server	3 years minimum from last date of entry	
SPD	Review minutes	SPR, SIS, DC	Hard copy/Server	3 years minimum from the last date of entry	
SPD	House/Team/Staff meeting minutes	SPR,SIS,DC,	Hard copy / Server	3 years	
SPD	Service user meeting/forum minutes	SPR,SIS,DC	Hard copy / Server	3 years	
PD	Fire Drill Evacuation Records	All	Manual	3 years	
PD	Contract with Local Authority (placement agreements)	SPR, SIS, Admin	Hard copy/Server	6 years	
PD	Service User Contract with Scotts	SPR, DC, Admin	Hard copy/Server	6 years	
PD	Tenancy Agreements	SIS, Admin	Hard copy/ Server	6 years	
PD	Financial Records	SPR, SIS	Hard copy	6 years	
SPD	Care Management Care Plan and Matrix	SPR,SIS,DC	Hard copy / Server	6 years from last date of entry	
SPD	Scott's Service User Needs Assessment	SPR,SIS	Hard copy / Server	6 years from last date of entry	

SPD	Care/ Support Plans	SPR, SIS, DC	Hard copy/Server	6 years from last date of entry	8 Years
SPD	Dairies/ Contact Sheets/ Daily Records	SPR, SIS,DC	Hard copies	6 years from the last date of entry	8 Years
SPD	Medical Records	SPR, SIS,DC	Hard copy/ Server	6 years from the last date of entry	8 years
SPD	Incident Records	SPR,SIS,DC	Hard copy/ Server	6 years from the last date of entry	10 years serious 20 years
SPD	Accident Records, Notifiable diseases and dangerous occurrences	SPR, SIS,DC	Hard copy	6 years from the last date of entry 12 years if industrial accident	10 years serious 20 years
SPD	Near Miss Record	SPR,SIS,DC	Hard copy	6 years	
SPD	Concern Record	SPR,SIS,DC	Hard copy	6 years	
SPD	Restraint Records			6 years	
SPD	DOLS Applications	SPR,SIS	Server	6 years	
SPD	CQC Notifications- Not Abuse	SPR,SIS	Server	6 Years	
SPD	Weight Charts	SPR	Manual	6 years	
SPD	Nutrition Records	SPR	Manual	6 years	
SPD	Fluid Charts	SPR	Manual	6 years	
PD	Record of Money / Valuables	SPR	Server	6 years	
SPD	Abuse Allegations or Incidents and all action taken including CQC/LA Notifications	SPR,SIS,DC	Server	50 years	
SPD	Copies of relevant information and accompanying correspondence relating to abuse, assault or molestation of/by a service user	SPR,SIS,DC	Hard copy/ Server	50 years	

Staff, Volunteers, Contractors, Outside Agency

Staff Data Retention Period

	Document/ Record	Department	Storage	Retention period
PD	Car Insurance details	HR		Keep latest Insurance certificate
PD	IT agreement	HR		Update annually- Form to be updated
PD	Unsuccessful applicant (short listing)- application forms Unsuccessful applicant (interview)- application form and interview notes	Admin	HR file/Server	6 months after shortlisting/ interview as could be required for a Tribunal or as a Subject Access Request
SPD	Hep B forms	Admin	HR file/Server	3 years
PD	Subject Access Request	Admin	Server	3 years
	P60	Admin	HR file/Server	3 years from the end of the Tax year it relates to
PD	Staff details sheets	All	HR File/ Copy held in SPR, SIS & DC	Update annually- keep 3 years
PD	Rotas	SIS,SPR,DC	Server/Hard Copy	6 years
PD	Payroll	Admin	Server	6 years
SPD	Accidents, Notifiable Disease and Dangerous Occurrences	SPR, SIS, DC, Admin	Hard Copy	Duration of employment + 6 months
SPD	Incidents	SPR, SIS, DC, Admin	Hard copy / server	Duration of employment + 6 months
PD	Annual Leave	SIS,SPR, DC, Admin, Maintenance	Server	On file for the duration of employment + 6 months
SPD	Staff Sickness Records	All	HR File	On file for the duration of employment + 6 months
PD	Salary increase letter	Admin	HR file/Server	On file for the duration of employment + 6 months

SPD	Medical Questionnaire	Admin	HR file/Server	On file for the duration of employment + 6 months
SPD	Staff Appraisal records	Admin	Server/Manual File	On file for the duration of employment + 6 months
SPD	Staff Supervision records	SIS, SPR,DC,ADMIN	Server /hard copy	On file for the duration of employment + 6 months
PD	Training records	All	Server/ HR File	On file for the duration of employment + 6 months
PD	Application form (successful applicant)	Admin	HR file/Server	50 Years
SPD	DBS number	Admin	HR file/Server	50 years
SPD	External Agency Staff information sheet	SPR, SIS	Server	50 years
PD	Engagement letters	Admin	HR file/Server	50 years
PD	References	Admin	HR file/Server	50 years
PD	I.D Verification records	Admin	HR file/Server	50 years
PD	Contracts of employment	Admin	HR file/Server	50 years
SPD	Pertinent related correspondence	Admin	HR file/Server	50 years
PD	Safeguarding Training Records	All	Server	50 years

Complaints

Personal Data	Department	Storage	Retention Period
Complaints	SPR, DC,SIS, Admin	Hard Copy/ Server	6 years

Children's Personal Data Retention Period

Document	Department	Storage	Retention Period
Name, Photo, contact details	DC	Hard Copy	50 years

Visitors

Record	Department	Storage	Retention Period
Visitors Book	SPR, DC, ADMIN	Hard Copy	7 years

Appendix 2

DATA BREACH REPORTING POLICY AND PROCEDURE

In accordance with the General Data Protection Regulation (GDPR), The Trust has introduced a Personal Data Breach Reporting Policy to comply with the regulatory reporting requirements and to set a procedural framework in line with The Trust's standards for data protection management.

Scope

The scope of the policy applies to security breaches in the processing of any the following categories of data:

- Personal data – information that relates to an individual and can be identified from that information.

- Special categories of personal data – information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

- Criminal records data – information about an individual's criminal convictions and/or offences and information relating to criminal allegations and proceedings.

The categories defined above will be referred to collectively as data throughout this policy and procedure document.

Processing is any use that is made of the data, including collecting, storing, amending, disclosing or storing it.

The policy and procedures set out apply to all of The Trust's Staff, Volunteers and Contractors (collectively referred to as an individual or individual for the purposes of this specific policy and procedure).

Data Breaches

A data breach is a security incident that has affected the confidentiality, integrity or availability of data. This is where personal data is lost, destroyed, corrupted or disclosed to unauthorised parties.

If an individual is any doubt about what constitutes a data breach, they should seek guidance from their manager. The Trust advocates diligence in relation to data processing and therefore encourages all staff to seek guidance and clarification in any circumstances where there is ambiguity.

Some examples

- The disclosure of data to the wrong recipient who is not authorised to receive such data. This may be by email or via other communication tools.
- The disclosure of data due to a lack of security measures, such as non-compliance with The Trust's data protection associated policies.
- Verbal disclosure of data to unauthorised parties. A breach may occur during informal discussions taking place within The Trust's services / departments or other locations during business and social events.
- System and technological failures resulting in security breaches.
- Theft of The Trust's or personal devices with stored data.
- Non-compliance with any of The Trust's procedures in relation to operational security.

Reporting Procedure
Where an individual believes they have made data breach, the incident must be reported immediately to the Senior Manager or to another Senior Manager in their absence or the CEO. The individual must provide the following information:

- The specific details about the incident including the categories and individual/s concerned, the specific data records concerned, when and how the breach occurred and details of any unauthorised recipients of the data.
- The date and time the breach was identified.
- Any other information to support the investigation, resolution and/or escalation of the incident.

Please note the CEO or appropriate authorised person will report incidents directly to the Information Commissioner as appropriate. In some cases, inform the affected individual where the breach is likely to result in a high risk of harm to the rights and freedoms of individuals. Individuals will be informed of the likely consequences of the breach and the mitigation measures that have been undertaken.

The Information Commissioner must be informed of any data breaches, posing a risk to the rights and freedoms of individuals, within 72 hours of the discovery. In order to ensure regulatory compliance, adherence to this policy and procedure is mandatory. Failure to do so could result in disciplinary action via The Trust's Disciplinary Policy.

Where the Trust processes personal data on behalf of a Local Authority/NHS, the CEO or appropriate authorised person will inform the Local Authority/ NHS of the breach, as soon as is reasonably possible, to enable the Local Authority/NHS, as the Controller, to report the data breach to the ICO within 72hours.

Appendix 3

Training

Staff training will cover as a minimum, the following areas-

1. How the Trust applies The Data Protection Principles.

2. Staff responsibilities when processing Personal Data for authorised purposes.

3. An explanation of the procedures and forms required by the Data Protection Policy.

4. Security of Personal Data-

- The correct use of passwords
- Use of screen savers
- Logging out from the server when the computer is not attended
- Secure storage of manual records
- Key holding
- Use of portable storage devices
- Disposal of Personal Data held on the server and in manual files/print outs

5. The need to obtain authorisation to transfer Personal Data outside of The Trust and the records to be completed.

6. Breach reporting.

7. Data Audits.

8. Retention schedules.