

# POL25 – Overarching Data Protection and GDPR Policy and Procedure

Human Resources - Performance & Discipline  
Serendipity Healthcare Ltd  
Unit 5 Millennium Way, Dunston, Chesterfield, Derbyshire, S41 8ND



## 1. Purpose

- 1.1 The purpose of this policy is to ensure that Serendipity Healthcare Ltd understands the key principles of the General Data Protection Regulation (GDPR).
- 1.2 This policy sets out the steps that need to be taken by Serendipity Healthcare Ltd to ensure that Serendipity Healthcare Ltd handles, uses and processes personal data in a way that meets the requirements of GDPR. It should be read alongside the suite of Serendipity Healthcare Ltd GDPR policies, procedures, and guidance.
- 1.3 This policy applies to all staff at Serendipity Healthcare Ltd who process personal data about other staff, Service Users, and any other living individuals as part of their role.
- 1.4 To support Serendipity Healthcare Ltd in meeting the following Key Lines of Enquiry:

WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?
WELL-LED	W3: How are the people who use the service, the public and staff engaged and involved?

- 1.5 To meet the legal requirements of the regulated activities that Serendipity Healthcare Ltd is registered to provide:
  - The Data Protection Act 2018
  - The General Data Protection Regulation 2016 (EU) 2016/679

## 2. Scope

The following roles may be affected by this policy:

- All staff

The following Service Users may be affected by this policy:

- Service Users

The following stakeholders may be affected by this policy:

- Family
- Commissioners
- Representatives
- Advocates
- NHS
- Local Authority
- External Health Professionals

## 3. Objectives

- 3.1 The objective of this policy is to ensure staff have a working knowledge into the principles and requirements of GDPR.
- 3.2 Alongside the suite of policies, procedures, and guidance available Serendipity Healthcare Ltd can demonstrate that appropriate steps are taken to ensure Serendipity Healthcare Ltd



complies with GDPR when handling and using personal data provided by both staff and Service Users.

- 3.3 This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention, and security of personal data.
- 3.4 This policy will assist with understanding the obligations of Serendipity Healthcare Ltd in respect of the rights of the staff and Service Users who have provided personal data and the steps Serendipity Healthcare Ltd should take if it breaches GDPR.

## 4. Policy

### 4.1 **GDPR Background**

GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998. Regardless of the impact of Brexit, GDPR will remain. GDPR provides greater protection to individuals and places greater obligations on organisations but can be dealt with in bite-size chunks to ensure that any impact on the provision of care and services is minimised.

- 4.2 All staff need to ensure the ways in which they handle personal data meet the requirements of GDPR.

### 4.3 Serendipity Healthcare Ltd's Approach to GDPR

Serendipity Healthcare Ltd is required to take a proportionate and appropriate approach to GDPR compliance. Serendipity Healthcare Ltd understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. We understand that if we process significant volumes of personal data, including special categories of data, or have unusual or complicated processes in place in terms of the way we handle personal data, we will consider obtaining legal advice specific to the processing we conduct and the steps we may need to take.

- 4.4 GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.

### 4.5 Process for Promoting Compliance at Serendipity Healthcare Ltd

To ensure Serendipity Healthcare Ltd compliance with GDPR, a suite of documents is available and should be read in conjunction with this overarching policy to provide a framework:

- GDPR – Key Terms Guidance
- GDPR - Key Principles Guidance
- GDPR - Processing Personal Data Guidance
- Appointing a Data Protection Officer Guidance
- Data Security and Data Retention Policy and Procedure
- Website Privacy and Cookies Policy and Procedure
- Subject Access Requests Policy and Procedure
- Subject Access Requests Process Map
- Subject Access Requests - Request Letter
- Rights of a Data Subject Guidance
- Breach Notification Policy and Procedure
- Breach Notification Process Map
- Fair Processing Notice Policy and Procedure
- Consent Form
- GDPR - Transfer of Data Guidance

## POL25 – Overarching Data Protection and GDPR Policy and Procedure

Human Resources - Performance & Discipline  
Serendipity Healthcare Ltd  
Unit 5 Millennium Way, Dunston, Chesterfield, Derbyshire, S41 8ND



- Privacy Impact Assessment (Privacy Notice) Policy and Procedure

### 4.6 Overview of Key Principles and Documents

The key principles and themes of each of the documents listed above are summarised below:

#### Key Terms

GDPR places obligations on all organisations that process personal data about a Data Subject. A brief description of those three key terms is included in the Definitions section of this document and are expanded upon in the Key Terms Guidance.

The requirements that Serendipity Healthcare Ltd need to meet vary depending on whether Serendipity Healthcare Ltd is a Data Controller or a Data Processor. We recognise that in most scenarios, Serendipity Healthcare Ltd will be a Data Controller. The meaning of Data Controller and Data Processor, together with the roles they play under GDPR, are explained in the Key Terms Guidance.

Special categories of data attract a greater level of protection, and the consequences for breaching GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This information is also covered in more detail in the Key Terms Guidance.

#### Key Principles

There are 6 key principles of GDPR which Serendipity Healthcare Ltd must comply with. These 6 principles

are very similar to the key principles that were set out in the Data Protection Act 1998. They are:

- Lawful, fair, and transparent use of personal data
- Using personal data for the purpose for which it was collected
- Ensuring that the personal data is adequate and relevant
- Ensuring that the personal data is accurate
- Ensuring that the personal data is only retained for as long as it is needed
- Ensuring that the personal data is kept safe and secure

These key principles are explained in more detail in the guidance entitled 'GDPR – Key Principles'. Serendipity Healthcare Ltd recognises that in addition to complying with the key principles, Serendipity Healthcare Ltd must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. We understand that we must also adopt 'privacy by design'. This means that data protection issues should be considered at the very start of a project, or engagement with a new Service User. Data protection should not be an after-thought. These ideas are also covered in more detail in the Key Principles Guidance.

#### Processing Personal Data

The position has been improved under GDPR in terms of the ability of care sector organisations to process special categories of data. The provision of health or social care or treatment or the management of health or social care systems and services is now expressly referred to as a reason for which an organisation is entitled to process special categories of data.

In terms of other types of personal data, Serendipity Healthcare Ltd must only process personal data if it is able to rely on one of a number of grounds set out in GDPR. The grounds which are most commonly relied on are:

- The Data Subject has given his or her consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract; and
- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

## POL25 – Overarching Data Protection and GDPR Policy and Procedure

Human Resources - Performance & Discipline  
Serendipity Healthcare Ltd  
Unit 5 Millennium Way, Dunston, Chesterfield, Derbyshire, S41 8ND



The grounds set out above and the impact of the changes made in respect of special categories of data are explained in more detail in the guidance entitled 'GDPR – Processing Personal Data'.

### **Data Protection Officers**

Serendipity Healthcare Ltd understands that some organisations will need to appoint a formal Data Protection Officer under GDPR (a “DPO”). The DPO benefits from enhanced employment rights and must meet certain criteria, so we recognise that it is important to know whether Serendipity Healthcare Ltd requires a DPO. This requirement is outlined in the policy and procedure on Data Protection Officers.

Whether or not Serendipity Healthcare Ltd needs to appoint a formal Data Protection Officer, Serendipity Healthcare Ltd will appoint a single person to have overall responsibility for the management of personal data and compliance with GDPR.

### **Data Security and Retention**

Two of the key principles of GDPR are data retention and data security.

- Data retention refers to the period for which Serendipity Healthcare Ltd keeps the personal data that has been provided by a Data Subject. At a high level, Serendipity Healthcare Ltd must only keep personal data for as long as it needs the personal data
- Data security requires Serendipity Healthcare Ltd to put in place appropriate measures to keep data secure

These requirements are described in more detail in the policy and procedure entitled Data Security and Data Retention.

### **Website Privacy and Cookies Policy and Procedure**

Where Serendipity Healthcare Ltd collects personal data via a website, we understand that we will need a GDPR compliant website privacy policy. The privacy policy explains how and why personal data is collected, the purposes for which it is used and how long the personal data is kept. A template website policy is provided.

### **Subject Access Requests**

One of the key rights of a Data Subject is to request access to and copies of the personal data held about them by an organisation. Where Serendipity Healthcare Ltd receives a Subject Access Request, we understand that we will need to respond to the Subject Access Request in accordance with the requirements of GDPR. To help staff at Serendipity Healthcare Ltd understand what a Subject Access Request is and how they should deal with a Subject Access Request, a Subject Access Request Policy and Procedure is available to staff. A Serendipity Healthcare Ltd process map to follow when responding to a Subject Access Request, as well as a Subject Access Request letter template is also included.

### **The Rights of a Data Subject**

In addition to the right to place a Subject Access Request, Data Subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by Serendipity Healthcare Ltd. All rights of the Data Subject are covered in detail in the corresponding guidance.

## POL25 – Overarching Data Protection and GDPR Policy and Procedure

Human Resources - Performance & Discipline  
Serendipity Healthcare Ltd  
Unit 5 Millennium Way, Dunston, Chesterfield, Derbyshire, S41 8ND



### **Breach Notification Under GDPR**

We understand, that in certain circumstances, if Serendipity Healthcare Ltd breaches GDPR, we must notify the ICO and potentially any affected Data Subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to all staff, together with a process map for Serendipity Healthcare Ltd to follow if a breach of GDPR takes place is available.

We understand that this requirement is likely to have less impact on NHS organisations that are already used to reporting using the NHS reporting tool.

### **Fair Processing Notice and Consent Form**

Organisations are required to provide Data Subjects with certain information about the ways in which their personal data is being processed. The easiest way to provide that information is in a Fair Processing Notice. A Fair Processing Notice template is available for Serendipity Healthcare Ltd to use and adapt on a case-by-case basis.

The Fair Processing Notice sits alongside a consent form which can be used to ensure that Serendipity Healthcare Ltd obtains appropriate consent, particularly from the Service User to the various ways in which Serendipity Healthcare Ltd uses the personal data. The Consent Form contains advice and additional steps to take if the Service User is a child or lacks capacity.

#### **Transfer of Data**

If Serendipity Healthcare Ltd wishes to transfer personal data to a third party, we understand that we should put in place an agreement to set out how the third party will use the personal data. The transfer would include, for example, using a data centre in a non-EU country. If that third party is based outside the European Economic Area, we recognise that further protection will need to be put in place and other aspects considered before the transfer takes place. Guidance has been produced to explain the implications of transferring personal data in more detail.

### **Privacy Impact Assessments**

Serendipity Healthcare Ltd must carry out Privacy Impact Assessments each time it processes personal data in a way that presents a “high risk” for the Data Subject. Examples of when a Privacy Impact Assessment should be conducted are provided in the relevant policy and procedure. Given the volume of special categories of data that are frequently processed by organisations in the health and care sector, there are likely to be a number of scenarios which require a Privacy Impact Assessment to be completed. The Privacy Impact Assessment template may also be used to record any data protection incidents, such as breaches or 'near misses'.

#### **4.7 Compliance with GDPR**

Serendipity Healthcare Ltd understands that there are two primary reasons to ensure that compliance with GDPR is achieved:

- It promotes high standards of practice and Care, and provides significant benefits for staff and, in particular, Service Users
- Compliance with GDPR is overseen in the UK by the ICO. Under GDPR, the ICO has the ability to issue a fine of up to 20 million Euros (approximately £17,000,000) or 4% of the worldwide turnover of an organisation, whichever is higher. The potential consequences are therefore significant.

Serendipity Healthcare Ltd appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance. A one- off, minor breach may not attract the attention of the ICO but if Serendipity Healthcare Ltd persistently breaches GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special categories of data), it may be subject to ICO

## POL25 – Overarching Data Protection and GDPR Policy and Procedure

Human Resources - Performance & Discipline  
Serendipity Healthcare Ltd  
Unit 5 Millennium Way, Dunston, Chesterfield, Derbyshire, S41 8ND



enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of Serendipity Healthcare Ltd and our data protection policies and processes. Serendipity Healthcare Ltd realises that the ICO may also require Serendipity Healthcare Ltd to stop providing services, or to notify Data Subjects of the breach, delete certain personal data we hold or prohibit certain types of processing.

### 5. Procedure

- 5.1 All staff should review the GDPR policies, procedures, and guidance that will be produced over the next few months.
- 5.2 Serendipity Healthcare Ltd will nominate a person or team to be responsible for data protection and GDPR compliance (if a formal Data Protection Officer is not required, somebody with an understanding of the requirements who can act as a day-to-day point of contact will be chosen).
- 5.3 The Registered Manager should ensure all staff understand the policies and procedures provided, including how to deal with a Subject Access Request and what to do if a member of staff breaches GDPR.
- 5.4 The Registered Manager will consider providing training internally about GDPR (in particular, the Key Principles of GDPR) to all staff members.
- 5.5 Serendipity Healthcare Ltd will delete any personal data that Serendipity Healthcare Ltd no longer needs, based on the results of the audit conducted, taking into account any relevant guidance, such as the Records Management Code of Practice for Health and Social Care 2016.
- 5.6 Serendipity Healthcare Ltd will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with GDPR.
- 5.7 Serendipity Healthcare Ltd will, if necessary, finalise and circulate a Fair Processing Notice to Service Users.
- 5.8 Serendipity Healthcare Ltd will ensure proper consent is obtained from each Service User in line with GDPR regulations (the Consent Form provided can be used for this purpose). Serendipity Healthcare Ltd will review the additional steps that Serendipity Healthcare Ltd should be taken to ensure that Serendipity Healthcare Ltd obtains consent from parents, guardians, carers, or other representatives where Serendipity Healthcare Ltd works with children or those who lack capacity.
- 5.9 Serendipity Healthcare Ltd will ensure that processes and procedures are in place to respond to requests made by Data Subjects (including Subject Access Requests) and to deal appropriately with any breaches or potential breaches of GDPR.
- 5.10 The Registered Manager will maintain a log of decisions taken and incidents that occur in respect of the personal data processed by Serendipity Healthcare Ltd using the Serendipity Healthcare Ltd Privacy Impact Assessment template.



## 6 Definitions

### 6.1 Data Subject

- The individual about whom Serendipity Healthcare Ltd has collected personal data

### 6.2 Data Protection Act 2018

- The Data Protection Act 2018 is a United Kingdom Act of Parliament that updates data protection laws in the UK. It sits alongside the General Data Protection Regulation and implements the EU's Law Enforcement Directive

### 6.3 GDPR

- General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It was adopted on 14 April 2016 and after a two-year transition period became enforceable on 25 May 2018

### 6.4 Personal Data

- Any information about a living person including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV, and special categories of data, defined below

### 6.5 Process or Processing

- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending, or transferring it. You do not need to be doing anything actively with the personal data – at the point you collect it, you are processing it

Reviewed 26.01.2022

Lisa Ward

HR Manager