GDPR03 - Data Security and Data Retention Policy and Procedure

Policy Review Sheet

Review Date: 07/03/18 **Policy Last Amended:** 07/03/18

Next planned review in 12 months, or sooner as required.

Note: The full policy change history is available in your online management system.

Business Impact:	Low	Medium	High	Critical
			X	
These changes require action as soon as possible. Changes include fixed implementation dates which are detailed within the policy.				

Reason for this review:	New Policy
Were changes made?	Yes
Summary:	This policy explains the key GDPR principles relating to data security and data retention and will assist organisations to review whether their current policies and procedures are sufficient, or whether they need updating.
Relevant Legislation:	• General Data Protection Regulation 2016 • Data Protection Act 2018
Underpinning Knowledge - What have we used to ensure that the policy is current:	• GOV.UK, (2018), *About the IG Toolkit*. [Online] Available from: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf [Accessed: 07/03/2018] • Department of Health & Social Care and NHS England, (2018), *2017/18 Data Security and Protection Requirements*. [Online] Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-_1.pdf [Accessed:07/03/2018] • Home Office, (2018), *An Employer's Guide to Right to Work Checks*. [Online] Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/638349/Employer_s_guide_to_right_to_work_checks_-August_2017.pdf [Accessed: 07/03/2018] • NHS DIGITAL,, (2018), *Records Management Code of Practice for Health and Social Care 2016*. [Online] Available from: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for- Health-and-Social-Care-2016 [Accessed: 07/03/2018]
Suggested action:	• Impact assessment/action plan • Discuss in supervision sessions • Notify relevant staff of changes to policy • Encourage sharing the policy through the use of the QCS App • Establish process to confirm the understanding of relevant staff • Establish training sessions for staff • Arrange specific meetings to discuss the policy changes and implications • Ensure that the policy is on the agenda for all team meetings and staff handovers

GDPR03 - Data Security and Data Retention Policy and Procedure

1. Purpose

1.1 The purpose of this policy is to ensure that Thistle Manor, Roefield Specialist Care Limited and all its staff understand the principles set out in GDPR in relation to data retention and data security.

1.2 By reviewing this policy, Thistle Manor, Roefield Specialist Care Limited will be able to consider appropriate retention periods for the personal data it processes.

1.3 This policy will enable Thistle Manor, Roefield Specialist Care Limited and all staff working at Thistle Manor, Roefield Specialist Care Limited to review the policies and procedures they have in place to ensure that personal data they process is kept secure and properly protected from unlawful or unauthorised processing and accidental loss, destruction or damage.

1.4 To support Thistle Manor, Roefield Specialist Care Limited in meeting the following Key Lines of Enquiry:

Key Question	Key Line of Enquiry (KLOE)
WELL-LED	W2: Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?

1.5 To meet the legal requirements of the regulated activities that Thistle Manor, Roefield Specialist Care Limited is registered to provide:

- General Data Protection Regulation 2016
- Data Protection Act 2018

2. Scope

2.1 The following roles may be affected by this policy:

- **All staff**

2.2 The following people may be affected by this policy:

- **Service Users**

2.3 The following stakeholders may be affected by this policy:

- **Family**
- **Advocates**
- **Representatives**
- **Commissioners**
- **External health professionals**
- **Local Authority**
- **NHS**

3. Objectives

3.1 The objective of this policy is to enable Thistle Manor, Roefield Specialist Care Limited to ensure its data retention and data security policies are GDPR compliant.

3.2 This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

GDPR03 - Data Security and Data Retention Policy and Procedure

4. Policy

4.1 Data Retention

As a general principle, Thistle Manor, Roefield Specialist Care Limited will not keep (or otherwise process) any personal data for longer than is necessary. If Thistle Manor, Roefield Specialist Care Limited no longer requires the personal data once it has finished using it for the purposes for which it was obtained, it will delete the personal data.

4.2 Thistle Manor, Roefield Specialist Care Limited may have legitimate business reasons to retain the personal data for a longer period. This may include, for example, retaining personnel records in case a claim arises relating to personal injury caused by Thistle Manor, Roefield Specialist Care Limited that does not become apparent until a future date. Thistle Manor, Roefield Specialist Care Limited should consider the likelihood of this arising when it determines its retention periods - the extent to which medical treatment is provided by Thistle Manor, Roefield Specialist Care Limited will, for example, affect the likelihood of Thistle Manor, Roefield Specialist Care Limited needing to rely on records at a later date.

4.3 Thistle Manor, Roefield Specialist Care Limited may be required to retain personal data for a specified period of time to comply with legal or statutory requirements. These may include, for example, requirements imposed by HMRC in respect of financial documents, or guidance issued by the Home Office in respect of the retention of right to work documentation (see "Underpinning Knowledge" section).

4.4 Thistle Manor, Roefield Specialist Care Limited understands that claims may be made under a contract for 6 years from the date of termination of the contract, and that claims may be made under a deed for a period of 12 years from the date of termination of the deed. Thistle Manor, Roefield Specialist Care Limited may therefore consider keeping contracts and deeds and documents and correspondence relevant to those contracts and deeds for the duration of the contract or deed plus 6 and 12 years respectively.

4.5 Thistle Manor, Roefield Specialist Care Limited will consider how long it needs to retain HR records. Thistle Manor, Roefield Specialist Care Limited may choose to separate its HR records into different categories of personal data (for example, health and medical information, holiday and absence records, next of kin information, emergency contact details, financial information) and specify different retention periods for each category of personal data. Thistle Manor, Roefield Specialist Care Limited recognises that determining separate retention periods for each element of personal data may be more likely to comply with GDPR.

Thistle Manor, Roefield Specialist Care Limited may decide, however, that separating its HR records into different elements is not practical, and that it can determine a sensible period of time for which to keep the HR records in their entirety. The period of time that is appropriate may depend on the likelihood of a claim arising in respect of that employee in the future. If, for example, Thistle Manor, Roefield Specialist Care Limited is concerned that an employee may suffer personal injury as a result of its employment with Thistle Manor, Roefield Specialist Care Limited, Thistle Manor, Roefield Specialist Care Limited may choose to retain its HR records for a significant period of time. If any such claim is unlikely, Thistle Manor, Roefield Specialist Care Limited may choose to retain its files for 6 or 12 years (depending on whether the arrangement entered into between Thistle Manor, Roefield Specialist Care Limited and the employee is a contract or a deed).

4.6 Thistle Manor, Roefield Specialist Care Limited will consider for how long it is required to keep records relating to Service Users. In doing so, Thistle Manor, Roefield Specialist Care Limited will consider the data retention guidelines provided by the NHS, if applicable. Those guidelines can be accessed by using the link in the "Underpinning Knowledge" section.

If the NHS guidelines don't apply to Thistle Manor, Roefield Specialist Care Limited, Thistle Manor, Roefield Specialist Care Limited will determine an appropriate retention policy for Service User personal data. Thistle Manor, Roefield Specialist Care Limited may choose to retain personal data for at least 6 years from the end of the provision of services to the Service User, in case a claim arises in respect of the services provided.

4.7 Irrespective of the retention periods chosen by Thistle Manor, Roefield Specialist Care Limited, Thistle Manor, Roefield Specialist Care Limited will ensure that all personal data is kept properly secure and protected for the period in which it is held by Thistle Manor, Roefield Specialist Care Limited. This applies in particular to special categories of data.

GDPR03 - Data Security and Data Retention Policy and Procedure

4.8 Thistle Manor, Roefield Specialist Care Limited will record all decisions taken in respect of the retention of personal data. Thistle Manor, Roefield Specialist Care Limited recognises that if the ICO investigates Thistle Manor, Roefield Specialist Care Limited's policies and procedures, a written record of the logic and reasoning behind the retention periods adopted by Thistle Manor, Roefield Specialist Care Limited will assist Thistle Manor, Roefield Specialist Care Limited's position.

4.9 Thistle Manor, Roefield Specialist Care Limited will implement processes for effectively destroying and/or deleting personal data at the end of the relevant retention period. Thistle Manor, Roefield Specialist Care Limited will consider whether personal data stored on computers, including in emails, is automatically backed up and how to achieve deletion of those backups or ensure that the archived personal data is automatically deleted after a certain period of time. Thistle Manor, Roefield Specialist Care Limited will consider circulating guidance internally to encourage staff to regularly delete their emails.

Thistle Manor, Roefield Specialist Care Limited will introduce policies relating to the destruction of hard copies of documents, including by placing the documents in confidential waste bins or shredding them.

4.10 Data Security

Thistle Manor, Roefield Specialist Care Limited will take steps to ensure the personal data it processes is secure, including by protecting the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.11 Thistle Manor, Roefield Specialist Care Limited understands that all health and care organisations, as detailed below, are required to comply with the Data Security and Protection Toolkit. A link to an explanatory guidance note is included in the "Underpinning Knowledge" section. Compliance with the Data Security and Protection Toolkit facilitates compliance with GDPR.

Thistle Manor, Roefield Specialist Care Limited understands that the following types of organisation must comply with the Data Security and Protection Toolkit:

- Organisations contracted to provide services under the NHS Standard Contract
- Clinical Commissioning Groups
- General Practices that are contracted to provide primary care essential services
- Local authorities and social care providers must take a proportionate response to the new toolkit:
    - Local authorities should comply with the toolkit where they provide adult social care or public health and other services that receive services and data from NHS Digital, or are involved in data sharing across health and care where they process confidential personal data of Service Users who access health and adult social care services
    - Social care providers who provide care through the NHS Standard Contract should comply with the toolkit. It is also recommended that social care providers who do not provide care through the NHS Standard Contract consider compliance with the toolkit as this will help to demonstrate compliance with the ten security standards and GDPR

4.12 Thistle Manor, Roefield Specialist Care Limited will implement and embed the use of policies and procedures to ensure personal data is kept secure. The suggestions below apply in addition to the steps Thistle Manor, Roefield Specialist Care Limited is required to take pursuant to the Data Security and Protection Toolkit, if the toolkit applies to Thistle Manor, Roefield Specialist Care Limited.

For paper documents, these will include, where possible:

- Keeping the personal data in a locked filing cabinet or locked drawer when it is not in use
- Adopting a "clear desk" policy to ensure that personal data is not visible or easily retrieved
- Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Redacting personal data from documents where possible
- Ensuring documents containing personal data are placed in confidential waste bins or shredded at the end of the relevant retention period

GDPR03 - Data Security and Data Retention Policy and Procedure

For electronic documents, the measures taken by Thistle Manor, Roefield Specialist Care Limited will include, where possible:

- Password protection or, where possible, encryption
- Ensuring documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them
- Ensuring ongoing confidentiality, integrity and reliability of systems used online to process personal data (this may require a review of IT systems and software currently used by Thistle Manor, Roefield Specialist Care Limited)
- The ability to quickly restore the availability of and access to personal data in the event of a technical incident (this may require a review of IT systems and software currently used by Thistle Manor, Roefield Specialist Care Limited)
- Taking care when transferring documents to a third party, ensuring that the transfer is secure and the documents are sent to the correct recipients

Thistle Manor, Roefield Specialist Care Limited will ensure that all business phones, computers, laptops and tablets are password protected.

Thistle Manor, Roefield Specialist Care Limited will encourage staff to avoid, storing personal data on portable media such as USB devices. If the use of portable media can't be avoided, Thistle Manor, Roefield Specialist Care Limited will ensure that the devices it uses are encrypted or password protected and that each document on the device is encrypted or password protected.

4.13 Thistle Manor, Roefield Specialist Care Limited will implement guidance relating to the use of business phones and messaging apps. Thistle Manor, Roefield Specialist Care Limited understands that all personal data sent via business phones, computers, laptops and tablets may be captured by GDPR, depending on the content and context of the message. As a general rule, Thistle Manor, Roefield Specialist Care Limited will ensure that staff members only send personal data by text or another messaging service if they are comfortable that the content of the messages may be captured by GDPR and may be provided pursuant to a Subject Access Request (staff should refer to the Thistle Manor, Roefield Specialist Care Limited Subject Access Policy and Procedure for further details).

4.14 Thistle Manor, Roefield Specialist Care Limited will ensure that all staff are aware of the importance of keeping personal data secure and not disclosing it on purpose or accidentally to anybody who should not have access to the information. Thistle Manor, Roefield Specialist Care Limited will provide training to staff if necessary. Thistle Manor, Roefield Specialist Care Limited will consider in particular, the likelihood that personal data, including special categories of data, will be removed from Thistle Manor, Roefield Specialist Care Limited's premises and taken to, for example, Service Users' homes and residences. Thistle Manor, Roefield Specialist Care Limited will ensure that all staff understand the importance of maintaining the confidentiality of personal data away from Thistle Manor, Roefield Specialist Care Limited's premises and take care to ensure that the
personal data is not left anywhere it could be viewed by a person who should not have access to that personal data.

4.15 Thistle Manor, Roefield Specialist Care Limited will adopt policies and procedures in respect of recognising, resolving and reporting security incidents including breaches of GDPR. Thistle Manor, Roefield Specialist Care Limited understands that it may need to report breaches to the ICO and to affected Data Subjects, as well as to CareCERT as Thistle Manor, Roefield Specialist Care Limited is required to comply with the Data Security and Protection Toolkit.

4.16 Thistle Manor, Roefield Specialist Care Limited will adopt processes to regularly test, assess and evaluate the security measures it has in place for all types of personal data.

4.17 Privacy By Design

Thistle Manor, Roefield Specialist Care Limited will take into account the GDPR requirements around privacy by design, particularly in terms of data security.

4.18 Thistle Manor, Roefield Specialist Care Limited understands that privacy by design is an approach set out in GDPR that promotes compliance with privacy and data protection from the beginning of a project. Thistle Manor, Roefield Specialist Care Limited will ensure that data protection and GDPR compliance is always at the forefront of the services it provides, and that it won't be treated as an afterthought.

4.19 Thistle Manor, Roefield Specialist Care Limited will comply with privacy by design requirements by, for example:

GDPR03 - Data Security and Data Retention Policy and Procedure

- Identifying potential data protection and security issues at an early stage in any project or process, and addressing those issues early on; and
- Increasing awareness of privacy and data protection across Thistle Manor, Roefield Specialist Care Limited, including in terms of updated policies and procedures adopted by Thistle Manor, Roefield Specialist Care Limited

4.20 Thistle Manor, Roefield Specialist Care Limited will conduct Privacy Impact Assessments to identify and reduce the privacy and security risks of any project or processing carried out by Thistle Manor, Roefield Specialist Care Limited. A template Privacy Impact Assessment is available within the Thistle Manor, Roefield Specialist Care Limited Initial Privacy Impact Assessment Policy and Procedure.

5. Procedure

5.1 Thistle Manor, Roefield Specialist Care Limited will consider data retention and data security issues and concerns at the beginning of any project (whether the project is the introduction of a new IT system, a new way of working, the processing of a new type of personal data or anything else that may affect Thistle Manor, Roefield Specialist Care Limited's processing activities). Thistle Manor, Roefield Specialist Care Limited appreciates that this is key for complying with the privacy by design requirements in GDPR.

5.2 Thistle Manor, Roefield Specialist Care Limited will review the periods for which it retains all the personal data that it processes.

5.3 Thistle Manor, Roefield Specialist Care Limited will, if necessary, adopt new policies and procedures in respect of data retention and will circulate those policies and procedures to all staff. Thistle Manor, Roefield Specialist Care Limited will consider providing training to staff in respect of data retention.

5.4 Thistle Manor, Roefield Specialist Care Limited will review the security measures currently in place in respect of all the personal data it processes.

5.5 Thistle Manor, Roefield Specialist Care Limited will document the decisions it takes, and the logic and reasoning behind those decisions, in respect of both data retention and data security. Thistle Manor, Roefield Specialist Care Limited will keep a record of all policies and procedures it implements to demonstrate its compliance with GDPR.

6. Definitions

6.1 CareCERT

- The Care Computing Emergency Response Team, developed by NHS Digital. CareCERT offers advice and guidance to support health and social care organisations to respond to cyber security threats

6.2 Data Subject

- The individual about whom Thistle Manor, Roefield Specialist Care Limited has collected personal data

6.3 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

6.4 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 trasition period became enforceable on 25 May 2018

6.5 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

GDPR03 - Data Security and Data Retention Policy and Procedure

6.6 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

6.7 Special Categories of Data

- Has an equivalent meaning to "Sensitive Personal Data" under the Data Protection Act 2018. Special categories of data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views

Key Facts - Professionals

Professionals providing this service should be aware of the following:

- Anybody who processes personal data on behalf of Thistle Manor, Roefield Specialist Care Limited should be made aware of and should comply with Thistle Manor, Roefield Specialist Care Limited's policies in respect of data retention and data security
- All personal data will be kept securely
- All retention periods need to be documented and justified
- Thistle Manor, Roefield Specialist Care Limited has effective and robust processes for destroying data
- Thistle Manor, Roefield Specialist Care Limited will comply with the Data Security and Protection Toolkit when necessary
- Electronic devices will be password protected to aid security
- Documents containing personal data are only shared with people who need to know the content
- Personal data will not be kept longer than necessary
- Personal data will be deleted when no longer needed
- Personal data may be held for longer than needed for the purposes of processing if there are justified reasons such as to meet regulations, insurance or other statutory requirements
- Retention periods are the decision of Thistle Manor, Roefield Specialist Care Limited, but guidance will be sought.

Key Facts - People Affected by The Service

People affected by this service should be aware of the following:

- Thistle Manor, Roefield Specialist Care Limited will implement and embed the use of policies and procedures to ensure that all personal data processed about people affected by the services provided by Thistle Manor, Roefield Specialist Care Limited, including Service Users, is retained and is kept secure and protected in accordance with GDPR