DATA PROTECTION POLICY & PROCEDURES

Version Number 1.1

Written: 13.06.2018

Review Period: Annually

Policy Responsibilities	
Initial document creation:	REGISTERED MANAGER, PROVIDER
Implementation:	Management team, nominated data protection officer
Reviewal:	Annual
Relevant standards/ guidance:	NHS Digital – GDPR Guidance Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17
Related Documents:	Record Keeping Policy Business Continuity Plan

Revisions to Policy & Procedures					
Version	**Page Number/ Section**	**Description of Changes Made**	**Written/ Reviewed By**	**Approved By**	**Date Approved**
1.0	All	Document Created	B.Hawkins / V.Ricketts	V.Ricketts / B.Hawkins	13.06.2018
1.1	All	Business Continuity Plan created	V.Ricketts	B.Hawkins	22.06.2019
1.1	All	None	V.Ricketts	B.Hawkins	04.07.2020
1.1	All	None	V.Ricketts	B.Hawkins	11.06.2021
1.2	All	Document reviewed, Regulation 17 added into policy underpinning New online training platform implemented DSPT published with added measures Mention of use of nhs.net secure account	V.Ricketts	B.Hawkins	18.06.2022

Contents

(All other appendices are in separate files)

1.0 INTRODUCTION

This Data Protection Policy is the overarching policy for data security and protection for Five Gables Care Home (hereafter referred to as "us", "we", or "our").

2.0 PURPOSE

The purpose of the Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the General Data Protection Regulations (2016) and the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy covers:

- → Our data protection principles and commitment to common law and legislative compliance
- → Procedures for maintaining the accuracy of data (including the correction of errors)
- → Procedures for data protection by design and by default
- → Data security and access procedures.

3.0 SCOPE

This policy includes in its scope all data which is stored, recorded or transferred either in hardcopy or digital copy and of which we can reasonably be stated to be either the data controller or data processor, this includes special categories of data.

This policy applies to all staff, including temporary staff and contractors.

4.0 PRINCIPLES

We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012. We will establish and maintain policies to ensure compliance with the GDPR, Human Rights Act 1998, the common law duty of confidentiality and the forthcoming Data Protection Act 2018, and all other relevant legislation. We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent.

Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time by informing a member of management. We ensure that it is as easy to withdraw as to give consent.

We acknowledge our accountability in ensuring that personal data shall be:

- → Processed lawfully, fairly and in a transparent manner
- → Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- → Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)
- → Accurate and kept up to date
- → Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’)
- → Processed in a manner that ensures appropriate security of the personal data

We uphold the personal data rights outlined in the GDPR:

- → The right to be informed
- → The right of access
- → The right to rectification
- → The right to erasure
- → The right to restrict processing
- → The right to data portability
- → The right to object
- → Rights in relation to automated decision making and profiling

5.0 ROLES AND RESPONSIBILITIES

5.1 Data Protection Officer (DPO)

Our designated Data Protection officer is BRIAN HAWKINS. He can be contacted via email at mail@fivegablescarehome.com or by phone on 01202 875130. The key responsibilities of the DPO are:

- Overseeing changes to systems and processes
- Monitoring compliance with the GDPR
- Assessing and reducing data protection risks
- Reporting on data protection and compliance with legislation to the registered manager
- Liaising, if required, with the Information Commissioner's Office (ICO)

5.2 Registered Manager

It is the responsibility of the registered manager to:

- Ensure that there are effective policies and procedures in place, which are reviewed and kept up to date, in order to allow the company to deal with data protection.
- Ensure that the Data Protection & Security Toolkit is kept updated and published in a timely manner
- Ensure that all staff are appropriately trained in data protection and security
- Audit and monitor day-to-day measures to implement data protection and security within the setting
- Use nhs.net secure email account for communication of any sensitive and/or confidential material

5.3 Care Home Workers

It is the responsibility of care home workers to:

- Work in accordance with company, local and national policies, guidance, rules and procedures
- Speak to management if they feel that they require further support or training in any areas
- Ensure that they maintain data protection at all times
- Report any suspected data breaches to the DPO

6.0 DATA ACCURACY PROCEDURE

We commit to ensuring that we comply with the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17 that we will "maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided".

We ensure accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

- **Authentic** – i.e. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed.
- **Reliable** – i.e. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records.
- **Integrity** – i.e. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified.
- **Useable** – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record.

The principal purpose of service user records is to record and communicate information about the individual and their care. The principal purpose of staff records is to record employment details for payroll and business planning purposes.

To fulfil these purposes, we:

- Use standardised structures, forms and layouts for the contents of records
- Ensure documentation reflects the continuum of care, that all care is person centred and that care records are viewable in chronological order
- Provide a clearly written care plan when care is being delivered by several members of the team, and we ensure that records are maintained and updated, and shared with everyone involved
- Train staff on the creation and use of records
- Have implemented a procedure that enables service users to have easy access to their records, in a format which they can understand (where possible)

All staff who record information - whether hardcopy or electronic - have a contractual responsibility to ensure that the data is accurate and as complete as possible. This responsibility extends to any system the staff member has access to.

7.0 PROCEDURES FOR THE CORRECTION OF ERRORS

In-line with national legislation individuals have the right to have access to their personal data which we process and store. Citizens/service users have the right to the rectification of said records in the instance that their records are inaccurate or incomplete. When there are errors which need correcting in care planning documents, this will usually be done as part of the regular care plan review process (at least once a month).

Where at all possible, in the instance that we have appropriately shared that individual's records with any third-party we will inform this third-party of the rectification if appropriate.

In all cases we will respond to a request for rectification within one month. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.

In order to request for their records to be rectified service users or staff should contact the Data Protection Officer with the request for rectification. If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.

In the instance where the rectification request is refused, the reason will be explained in full and in writing within one month of the original request having been received.

A record of all rectification requests and outcomes will be kept in line with timeframes outlined in the Information Governance Alliance's Appendix 3 of the Record Management Code of Conduct for Health and Social Care 2016 (https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016). These records will be kept in our "GDPR Request Record". If the rectification is relating to a care planning document, then changes will be recorded on the Care Plan Agreement form.

All individuals who have their rectification request refused will be informed of their legal rights to complain to the ICO and to seek a judicial remedy.

All service users, or their legal representative, will be informed of this policy, as well as their other rights regarding their personal data, when they sign initial terms and conditions of residency with us.

8.0 DATA PROTECTION BY DESIGN AND BY DEFAULT

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will take into account the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.
We shall uphold the principles of data protection by design and by default from the beginning of any data processing.

All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.
We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

9.0 DATA SECURITY AND ACCESS

The information we store can be accessed in two ways; physically (in person) or digitally (e.g. on a computer). Depending on the method in question, the related security procedures will differ, as follows -

9.1 Physical Access Procedure

Physical access to records shall only be granted on a strict 'Need to Know' basis.

During their induction each staff member who requires access to confidential information for their job role will be trained on the safe handling of all information and will be taught the procedures which govern how data is used, stored, shared and organised in our organisation.

Our staff must retain personal and confidential information and data securely in locked storage when not in use, and keys should not be left in the barrels of filing cabinets and doors.

Secure information is stored in locked filing cabinets in the main office and outside office. All offices, when left unoccupied, must be locked unless all personal and confidential information has first been cleared off work stations/desks and secured in locked storage.

The Information Asset Register (IAR) will contain the location of all confidential and sensitive personal information.

We will risk assess each storage location to ensure that the data is properly secured. This risk assessment forms part of the IAR.

Current care planning records can be accessed by all care staff and management.

Outdated/previous care plan records can be accessed by management only.

Staff files can be access by management only (except for if a staff member wishes to view their own records).

9.2 Digital Access Procedure

Access shall be granted using the principle of 'Least Privilege'. This means that every program and every user of the system should operate using the least set of privileges necessary to complete their job.
Only management will be able to access sensitive material digitally.
We will ensure that each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.
During their induction each staff member who requires access to digital systems for their job role will be trained on the use of the system, given their user login details, and they will be required to sign to indicate that they understand the conditions of access.
In the instance that there are changes to user access requirements, these can only be authorised by the Data Protection Officer. The IAR will contain the location of all confidential and sensitive personal information which is digitally stored.
We will follow robust password management procedures and ensure that all staff are aware of good password management.
As soon as an employee leaves, all their system logons are revoked. As part of the employee termination process the Data Protection Officer is responsible for the removal of access rights from the computer system.

When not in use all screens will be locked, and a clear screen policy will be followed. There is guidance on clear screen policies here:
https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/clear-desk-and-screen

10.0 CONTINGENCY PLANS

In the event of data loss, the following systems and precautions are in place:

10.1 Loss of Digital Records

All digital records are backed up on to an external hard drive once a month. This hard drive is encrypted to prevent unauthorised access and is stored in a secure location away from the main site.

10.2 Loss of Hardcopies/Paper Files

Care Plans are also kept in digital format, so these can be replaced if they are lost. Files such as daily records, MAR charts, etc. are securely stored in a locked room/cabinet but cannot be easily replaced. However, this does not present a high risk to service users because loss of this information is unlikely to cause the care and services we provide to become unsafe.

All staff paper records are scanned and stored digitally (where possible). The original copies are then returned to the staff member or destroyed in line with our Record Keeping Policy.

11.0 POLICY UNDERPINNING

This policy is underpinned by the following:

- Record Keeping Policy – details the management of records from creation to disposal, this is inclusive of retention and disposal procedures
- Staff Contracts - provides staff with clear guidance on the disclosure of personal information
- Data Protection & Security Toolkit (online and linked with nhs.net secure email account

12.0 APPENDICES

All staff should be familiar with the following documents:

Document name	Location
The Care Certificate (Skills for Care)	http://www.skillsforcare.org.uk/Standards/Care-Certificate
NHS Digital – GDPR Guidance	https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance
The Record Keeping Policy	In the Five Gables Care Home Policies folder