Data Quality Policy

1. Introduction

1.1. This Data Quality Policy is ***Briarlea Care Home's*** (hereafter referred to as "us", "we", or "our") policy for the ensuring accuracy of information which we store and process.

2. Purpose

2.1. The availability of accurate and timely data is vital for the safety of the people we care for and the safe and responsible running of our organisation. This policy outlines the following procedures:

2.1.1. Procedures for ensuring data accuracy;

2.1.2. Procedures for correcting errors.

3. Scope

3.1. This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data;

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

4. Data accuracy procedures

4.1. 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";

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

4.2.1. 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;

4.2.2. 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;

4.2.3. 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;

4.2.4. Useable – i.e. the data can be located when it is required for use and its context is clear in a contemporaneous record.

4.3. 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.

4.4. To fulfil these purposes, we:

4.4.1. Use standardised structures and layouts for the contents of records;

4.4.2. Ensure documentation reflects the continuum of care, that all care is person centred and that care records are viewable in chronological order;

4.4.3. 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;

4.4.4. Train staff on the creation and use of records (see the Record Keeping Policy);

4.4.5. Have implemented a procedure that enables service users and staff to have easy access to their records where appropriate. This is outlined in the Record Keeping Policy.

4.5. 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.

5. Procedures for the correction of errors

5.1. In-line with national legislation, individuals have the right to have access to their personal data which we process and store. Citizens have the right to the rectification of said records in the instance that their records are inaccurate or incomplete.

5.2. 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.

5.3. 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.

5.4. To request for their records to be rectified service users or staff should contact us with the request for rectification either verbally or in writing**.** If the rectification is due to the record being incomplete, then the individual should also provide the supplementary information to update the record.

5.5. While we are assessing the request to rectify records, we will restrict processing of the data in question. This will be done in line with our Right to Restrict Processing Procedure as outlined in our Record Keeping Policy.

5.6. 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.

5.7. A record of all rectification requests and outcomes will be kept by the Data Security and Protection Lead in line with timeframes outlined in the NHS England Records Management Code of Practice.
https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

5.8. 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;

5.9. All staff will be informed of this policy in the staff handbook.

5.10. All service users, or their legal representative, will be informed of this policy, as well as their other rights as regards their personal data, when they sign initial contracts with us.

5.11. In order to process your request for rectification, you might be asked to provide identifying documents so that we can authenticate that it is appropriate for you to update your data.

6. Responsibilities

6.1. The Data Security and Protection Lead has overall responsibility for Data Quality policies and procedures being reviewed annually and for staff training in data quality and for monitoring data quality throughout the organisation. They also are responsible for responding to rectification requests and recording the outcome of any request.

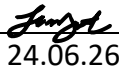
6.2. The Registered Manager is responsible for the quality of records and making sure that staff understand their commitments in ensuring data quality.

6.3. Every member of staff is individually responsible for the quality of data they personally record – whether on paper or electronically. Additionally, they are responsible for reporting any mistakes they do notice to the Data Security and Protection Lead.

6.4. Staff are aware that data accuracy and security is a contractual and legislative requirement and that breach of this policy might result in disciplinary action.

7. Approval

7.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Name	James Hunt, Director
Signature	
Reviewed on	24.06.26