Milewood
INDIVIDUAL CARE AND SUPPORT

Document name:	Data Protection Policy
Issue number:	1
Date issued:	June 2025
Next review date:	June 2026
Owner:	DPO

DATA PROTECTION POLICY

Contents

Introduction

As a social care provider, we handle a large amount of highly sensitive information, such as support plans and health action plans for the people who use our services and recruitment data for the people who work for us.
We cannot take personal data for granted, it's not a commodity we own: it is only ever on loan. Individuals have been given control by law, and we have been given the duty of care over it.

The UK Data Protection Act 2018 came into force in May 2018, which is based on the UK General Data Protection Regulations (UK-GDPR). This replaced the Data Protection Act 1998 and other existing Data Protection Laws to make them fit for the digital age in which ever-increasing personal data is being processed.

The Act sets standards for protecting personal data, gives people more control over the use of their data and assists in the preparation for a future outside of the EU.

Purpose

This policy sets out

- the requirements of the law
- how we will meet our legal obligations
- procedures for data protection by design and by default
- how we prevent data security breaches and how we react to them when prevention is not possible
- Procedures for ensuring data accuracy
- Procedures for correcting errors

Staff awareness and understanding of their responsibilities regarding the handling, collection, and retention of data will be core to the successful embedding of this policy.

Data accuracy and security is a contractual and legislative requirement and breach of this policy might result in disciplinary action.

Scope

This policy covers all staff employed either temporarily or permanently within the Milewood Group: Milewood Healthcare Limited, Care Network Solutions Limited, Elmcare Limited, Whitwell Park Care Home Limited, Walton Lodge Limited, MC Independent Care Initiatives Limited and Ambercare Limited (East Anglia)

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

Definitions

The UK GDPR applies to “Controllers”, “Processors” and “Data Protection Officers” and to certain types of information, specifically, “Personal Data” and “Sensitive Personal Data” referred to in the Act as Special Categories of Personal Data”.

“Controllers”

This role determines, on behalf of the organisation, the purposes, and means of processing personal data.

“Processors”

This role is responsible for processing personal data on behalf of a controller. The Act places specific legal obligations on us where we are a processor, e.g. you are required to keep and maintain records of personal data and processing activities. This role has legal liabilities if they are responsible for any breach.

“personal data”

Personal data is any information that relates to an identified or identifiable living individual (called a "data subject"). This includes information that can directly or indirectly identify someone.

Examples include:

- Name
- Email address
- Phone number
- IP address
- Location data
- Employee or customer ID
- Photos or CCTV footage

If the data can be used to identify someone, even when combined with other information, it counts as personal data.

“Special Categories of Personal Data”

Special category data is a subset of personal data that is considered more sensitive and therefore requires extra protection. The UK GDPR restricts how this data can be processed and requires a lawful basis under both Article 6 and Article 9 of the regulation.

This includes data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (used for identification)
- Health data
- Data about a person’s sex life or sexual orientation

This type of data is protected more strictly because misuse could lead to discrimination or harm to an individual's rights and freedoms

“Data breach”

A security incident in which the confidentiality, integrity or availability of data is compromised. A breach can either be purposeful or accidental.

Responsibilities

Senior Information Risk Officer (SIRO)

The SIRO has accountability for ensuring that effective systems and processes are in place to address the Information Governance agenda, including records and document management.

The SIRO is the overall owner of information risk within the organisation and acts as the focal point for information risk management in the organisation including resolution of any risk issues raised by Information Asset Owners.

The SIRO is the Chief Executive Officer, and can be contacted at martyn.heginbotham@milewood.co.uk

Data Protection Officer (DPO)

The DPO is responsible for monitoring compliance with data protection legislation and compliance with own own policies in relation to the personal data of living individuals.

The DPO will liaise, if required, with the Information Commissioner’s Office (ICO)

The DPO is the Head of Quality, Governance & Safeguarding and can be contacted at dataprotection@milewood.co.uk

All Managers

All managers are to make sure that their teams are aware of this policy and operate within it.

All Staff

All staff are responsible for reading this policy, understanding how it applies to their role and where to get further information.

All staff have a responsibility for the quality of data they personally record, whether on paper or electronically.

All staff must operate within the policy guidelines and report any concerns to their manager or Data Protection Officer.

Policy

We will be open and transparent with people we support 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 Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the UK-General Data Protection Regulation and all other relevant legislation.

We will establish and maintain policies for the controlled and appropriate sharing of personal data belonging to staff and people we support 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.

People we support can withdraw consent at any time as outlined in our Record Keeping Policy. We will ensure that it is as easy to withdraw as to give consent.

We will carry annual audits of our compliance with legal requirements.

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

- Processed lawfully, fairly and in a transparent manner
- Collected and used for specified, explicit and legitimate purposes
- Used in a way that is adequate, relevant and limited only what is necessary ('data minimisation')
- Accurate and kept up to date
- Kept for no longer than is necessary ('storage limitation')
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

We uphold the personal data rights outlined in the UK-GDPR:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

In line with legislation, we have a Data Protection Officer (DPO) who reports to the CEO. The DPO will be supported with the necessary resources to carry out their tasks and ensure that they can maintain expertise. The DPO will not be pressured on how to carry out DPO related tasks, and is protected from disciplinary action when carrying out the tasks associated with their role.

We complete the Data Security and Protection Toolkit on an annual basis and our publication status can be found here: https://www.dsptoolkit.nhs.uk/OrganisationSearch/A961

Data protection by design and by default

We will 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 consider 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 and during the planning and implementation of any new data process.

Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist.

All new systems used for data processing will have data protection built in from the beginning of the system change.

All existing data processing has been recorded on our Record of Processing Activities. Each process will be risk assessed and reviewed annually.

We will 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 will 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.

Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

Procedure

Data Security

Physical Access Procedures

- 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 data securely in locked storage when not in use and keys should not be left in the barrels of filing cabinets and doors.
- 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 confidential and sensitive personal information.

- Regional Operations Managers will ensure each storage location is risk assessed to ensure that the data is properly secured.
- Regional Operations Managers will ensure a record is kept of who has access to each storage location.
- An audit will be completed at least annually to ensure that information is secured properly and that access is restricted to those who have a legal requirement to use the information. The details of this audit are outlined in the Data Security Audit Procedures below.

Digital Access Procedures

- 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.
- 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.
- The use of group IDs is only permitted where they are suitable for the work carried out
- 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.
- A record is kept of all users given access to the system. The record will be retained by IT.
- In the instance that there are changes to user access requirements, these can only be authorised by a member of the senior leadership team
- The IAR will contain the location of confidential and sensitive personal information which is digitally stored.
- We will follow robust password management procedures
- As soon as an employee leaves, all their system logons are revoked
- As part of the employee termination process the senior leadership team is responsible for the removal of access rights from the computer system.
- The senior leadership team will review all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons which are identified are disabled immediately and deleted unless positively reconfirmed.
- When not in use all screens will be locked and a clear screen policy will be followed

Access Monitoring Procedures

The management of digital access rights is subject to regular compliance checks to ensure that these procedures are being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

Areas considered in the compliance check include whether:

- Allocation of administrator rights is restricted
- Access rights are regularly reviewed
- Whether there is any evidence of staff sharing their access rights
- Staff are appropriately logging out of the system
- Our password policy is being followed
- Staff understand how to report any security breaches

Data Security Audit Procedures

Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient controls. Audits of security and access arrangements within each area are to be conducted on an annual rolling programme.

Audits will be carried out as required by some or all of these methods:

- Unannounced spot checks to random work areas
- A series of interviews with managers and staff, where a department or area of the organisation have been identified for a confidentiality audit. These audits will be carried out by the Quality Team or Regional Operations Managers
- Based on electronic reports
- Based on electronic reports from support planning software or auditing of support plans

The following checks will be made during data security audits:

- The Information Asset Register has been reviewed, updated and signed off
- The Record of Processing Activities has been reviewed, updated and signed off
- Failed attempts to access confidential information
- Repeated attempts to access confidential information
- Access of confidential information by unauthorised persons
- Previous confidentiality incidents and actions, including disciplinary, taken
- Staff awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality
- Appropriate communications with people we support
- Appropriate recording and/or use of consent forms
- Appropriate allocation of access rights to confidential information, both hardcopy and digital
- Appropriate staff access to physical areas
- Storage of and access to filed hardcopy notes for people we support and information
- Correct process used to securely transfer personal information by post, fax or email
- Appropriate use and security of desktop computers and mobile devices in open areas
- Security applied to PCs, laptops and mobile electronic devices
- Evidence of secure waste disposal
- Appropriate transfer and data sharing arrangements are in place
- Security and arrangements for recording access to manual files both live and archive, *e.g.* storage in locked cabinets/locked rooms

Data Security Breach Procedures

To mitigate the risks of a security breach we will:

- Follow the Physical Access, Digital Access, Access Monitoring and Data Security Procedures
- Ensure our staff are trained to recognise a potential data breach whether it is a confidentiality, integrity or availability breach
- Ensure our staff understand the procedures to follow and how to escalate a security incident to the correct person in order to determine if a breach has taken place

What to do if you suspect a data breach has occurred

- The staff member who notices the breach, or potential breach, will complete a Data Security Incident Report Form (appendix B) without delay and inform their manager or on call manager if out of hours
- This form will be completed and emailed to the DPO or, if they are not available, to a member of senior management
- The DPO will complete the rest of the Incident Report Form and ensure the breach is investigated
- In the instance that the breach is a personal data breach and it is likely that there will be a risk to the rights and freedoms of an individual then the Information Commissioner's Office (ICO) will be informed as soon as possible, but at least within 72 hours of our discovery of the breach, via the DSPT Incident Reporting Tool (www.dsptoolkit.nhs.uk/incidents/);

As part of our report we will provide the following details:

- The nature of the personal data breach (i.e. confidentiality, integrity, availability)
- The approximate number of individuals concerned and the category of individual (e.g. employees, mailing lists, people we support)
- The categories and approximate number of personal data records concerned
- The name and details of our DPO
- The likely consequences of the breach
- A description of the measures taken, or which we will take, to mitigate any possible adverse effects.
    - The DPO will ensure that any individual is informed that their personal data has been breached if it is likely that there is a high risk to their rights and freedoms. We will inform them directly and without any undue delay
    - The data security breach will be marked on the IAR
    - A record of all personal data breaches will be kept including those breaches which the ICO were not required to be notified about

Data Quality

Data accuracy procedures

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 will 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

The principal purpose of records for people we support 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 will:

1. Use stand document-controlled forms and digital systems wherever possible
2. Ensure care is person centred and that care records are viewable in chronological order
3. Provide a clearly written support plan, ensure that records are maintained and updated, and share with everyone involved
4. Inform staff about how to create and use records (see the Record Keeping Policy)
5. Ensure people we support and staff can have easy access to their records where appropriate. This is outlined in the Record Keeping Policy and our Privacy Notice.
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.

Procedures for the correction of errors

1. In-line with national legislation, people have the right to have access to their personal data which we process and store. They also have the right to the rectification of their records if the records are inaccurate or incomplete.
2. Where possible, if we have shared that individual's records with any third-party we will inform this third-party of the rectification if appropriate.
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.
4. To request for their records to be rectified people we support or staff should contact us with the request for rectification either verbally or in writing. People we support can ask any member of staff to do this – if you get such a request ask advice from the DPO. If the rectification is due to the record being incomplete, then we will ask the individual to provide the supplementary information to update the record.
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 Record Keeping Policy.
6. If 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.
7. A record of all rectification requests and outcomes will be kept by the DPO
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
10. Regional Operations Managers will ensure that people we support, or their legal representative, are informed of this policy, as well as their other rights as regards their personal data, when they sign initial contracts with us.

11. In order to process a request for rectification, the individual might be asked to provide identifying documents so that we can authenticate that it is appropriate to update the data.

Data Security and Protection Toolkit (DSPT)

We update annually or when changes occur, our Data Security and Protection Toolkit (DSPT) to ensure it reflects our current data and cyber security arrangements, taking into account any changes and how we manage data throughout the year. We ensure the relevant staff are trained and competent to complete the toolkit.

Records

All records must be kept in line with legal requirements, the Record Keeping Policy and the Confidentiality & Disclosure of Information Policy.

Training

Staff must complete data protection and cyber security training at a level appropriate to their role.

Senior staff with specific data security responsibilities complete enhanced training. Training will be refreshed annually.

How we will let you know about the policy and put it into practice

The policy will be made available on Redcier and on SharePoint. It will be made available to all staff at induction and to existing staff via team meetings. Learning and development needs will be assessed via the supervision and appraisal process.

All staff have responsibility for making sure they read this policy, understand how it applies to their role and where to get further information.

Equality, diversity and inclusion

All staff are expected to deliver services in a manner which respects the individuality of each person using the service and treat people using services and members of the workforce respectfully, regardless of protected characteristics.

Staff will be mindful of people’s preferences in how they manage personal data.

How we will know the policy is working

Service Managers and Regional Operations Managers will monitor the implementation of and compliance with the policy, highlighting trends in practice and areas for improvement.

An annual internal audit will provide validation about compliance with the policy.

Related guidance and policies

Guide to the UK General Data Protection (UK GDPR):
https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR-1-0.pdf
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR/

Records Management Code of Practice for Health and Social Care 2016:
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

ICO Data Protection Self-Assessment:
https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/data-protection-self-assessment/

Direct Marketing Guidance:
https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/direct-marketing-guidance/

Guide to privacy and Electronic Communications Regulations (PECR):
https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/

Data Protection and the use of Criminal Offence Data for Employment and Education Purposes:
https://www.nacro.org.uk/

Regulation 20: Duty of candour - Care Quality Commission (cqc.org.uk)
https://www.cqc.org.uk/guidance-providers/all-services/regulation-20-duty-candour

Right of Access
https://ico.org.uk/right-of-access

Digital Care Hub: DSPT
https://www.digitalcarehub.co.uk/dspt/?mc_cid=7496c11fbb&mc_eid=2bc19b00d4

Transparency in Health and Social Care
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/transparency-in-health-and-social-care/

Related policies

- Safeguarding Adults
- Accessible Information and Communication
- Access to Records
- CCTV

- Confidentiality & Disclosure of information
- Consent
- Duty of Candour
- Record Keeping

Appendix A: Version control

Record of changes

The policy has been completely rewritten and the new template used.

Review cycle

This policy will be reviewed every year as part of a planned schedule, or sooner if there are changes to legislation or best practice.

Appendix B: Data Security Incident Report Form

In the event of a data security incident this form must be completed in full within 24 hours of the incident.

This form can be completed online here https://forms.office.com/e/gdfgrCMcg7 or via the QR code, or emailed to the Data Protection Officer at dataprotection@milewood.co.uk

Please complete ALL sections below

Date of incident	
Service/s involved	
Location of incident	
Type of data breach: **Digital** – e.g. Hacking, Virus, Ransomware, File corruption, phishing	

Electronics – e.g. lost laptop, phone, USB device, email sent in error **Verbal**- e.g. wrong information given over the phone **Paper** – e.g lost or misplaced file	

Incident Details:

Please state the facts only, including names of any staff involved and any contributing factors. Do **NOT** include any client details

Describe what happened?
How was the incident discovered?
When was the incident discovered?
What type of data was included in the breach? (e.g. Personal identifiers, health data, usernames or passwords, financial data, official documents, other personal data)
How many data subjects could be affected?
Which category of data subjects could be affected?
Have there been any consequences arisen from the breach so far?

What steps have been taken to minimise the impact of the breach and prevent reoccurrence?

Reporter Details:

Name	
Job Title	
Signature	

Data Protection Officer Use only:

Date report received	
Incident Log Number	
Actions taken	
Investigation and follow up completed (Date)	