Confidentiality Policy
The Heather Club
Effective Date: 17th January 2025

Introduction

The Heather Club is committed to protecting the privacy and confidentiality of all individuals involved in our work. As a charity providing services to adults with dementia and memory loss, we handle sensitive and personal information daily. This policy outlines the principles and procedures for maintaining confidentiality and ensuring that personal and sensitive data is handled in accordance with legal requirements and best practices.

Purpose

The purpose of this policy is to:

- Ensure that all personal, medical, and sensitive information about Members, staff, volunteers, and other individuals is kept confidential.
- Establish clear guidelines for how confidential information is handled, stored, shared, and disposed of.
- Comply with relevant data protection legislation, including the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).
- Promote a culture of respect for privacy and confidentiality within The Heather Club.

Scope

This policy applies to:

- All staff, volunteers, and trustees of The Heather Club.
- Any third parties who may have access to confidential information as part of their role (e.g., contractors, service providers).
- All personal, medical, and sensitive data collected and processed by The Heather Club as part of the provision of care and services at the club.

Definitions

1. Confidential Information

Any information that is not available to the general public and is related to the charity's operations, Members, staff, volunteers, or trustees. This includes:

- Personal details of Members (e.g., names, addresses, contact information).
- Medical and care information (e.g., health conditions, treatment plans, medication).
- Financial information (e.g., donations, fund-raising details).
- Employment information (e.g., staff contracts, performance reviews, disciplinary records).

2. Personal Data

Personal data refers to information that can identify an individual, either on its own or in combination with other data. Examples include names, contact details, and other personal identifiers.

Principles of Confidentiality

1. Respect for Privacy
• All personal information must be handled with the highest level of respect for privacy and dignity. Members' privacy and confidentiality must be upheld at all times, including in situations where they may be vulnerable due to dementia or memory loss.
2. Need-to-Know Basis
• Confidential information should only be shared on a need-to-know basis. Information should not be disclosed unless it is essential for the provision of care, service, or for a legitimate purpose under the law (e.g., safeguarding concerns, legal obligations).
3. Informed Consent
• Members must be informed about how their personal data will be used and provide consent where applicable. If a service user is unable to give consent, staff should act in the best interests of the individual, following legal or ethical guidance where necessary.
4. Secure Handling of Information
• Confidential information must be stored securely, whether it is in paper or digital form. Appropriate security measures must be in place to protect data from unauthorized access, loss, or theft.
• Paper records should be kept in locked cabinets, and digital records should be protected by passwords and encryption.
5. Respect for Staff and Volunteers' Privacy
• The personal information of staff, volunteers, and trustees must also be handled confidentially. This includes sensitive personal information such as health records, employment history, and disciplinary records.
6. Training and Awareness
• All staff and volunteers will receive training on the importance of confidentiality and data protection as part of their induction and on an ongoing basis. Regular updates and reminders will be provided to ensure awareness of best practices and legal obligations.

Handling of Confidential Information

1. Collection and Recording of Information
• Information should only be collected and recorded when necessary for the purpose of providing care, support, or services. This should be done in a clear, accurate, and timely manner.
• All staff and volunteers should ensure that any information they collect is relevant and up-to-date.
2. Storage of Information
• Personal, sensitive, or confidential information should be stored in a secure manner, whether it is in paper form or electronically.
• Electronic records should be protected with passwords, and access should be limited to authorised personnel.
• Paper records should be kept in locked cabinets, and access should be restricted to those who need it.
3. Sharing of Information
• Confidential information should only be shared with individuals or organisations who have a legitimate reason to access it (e.g., healthcare providers, family members,

or emergency services), and only with the consent of the individual concerned, unless there is a legal or safeguarding reason to disclose.
• If there is any doubt about whether information should be shared, staff should consult with the Club manager.

4. Email and Electronic Communication

• When sharing confidential information via email or other electronic methods, staff should ensure that sensitive information is encrypted or securely transmitted.
• Emails containing confidential information should only be sent to the intended recipient, and care should be taken to avoid sending information to unintended parties.

5. Disposal of Information

• Confidential information must be disposed of securely when it is no longer needed. Paper records should be shredded, and electronic records should be securely deleted.
• When disposing of hardware containing confidential information (e.g., computers, mobile devices), all data should be fully erased using appropriate data destruction methods.

Breaches of Confidentiality

1. Reporting Breaches

• If a breach of confidentiality occurs, it must be reported immediately to the Club Manager.
• All breaches will be investigated promptly, and corrective action will be taken to prevent further occurrences.

2. Disciplinary Action

• Any deliberate or negligent breach of confidentiality will be taken seriously and may result in disciplinary action, up to and including termination of employment or volunteer status.

3. Legal Consequences

• Breaches of confidentiality may also lead to legal action, especially if personal data is mishandled in violation of data protection laws such as the Data Protection Act 2018 or the UK GDPR. Employees or volunteers may be personally liable for the unauthorised disclosure of confidential information.

Data Protection and Legal Compliance

1. Data Protection Act 2018 and UK GDPR

• The Heather Club is committed to complying with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). Personal data will be collected, processed, and stored in compliance with these regulations.

2. Members' Rights

• Members have the right to access their personal data, correct inaccuracies, and request that their information be deleted in certain circumstances. Requests for access to personal data should be directed to the charity's data protection officer.

Monitoring and Review

• This policy will be reviewed annually or in response to significant changes in data protection laws, regulations, or charity practices.

- Regular audits will be conducted to ensure compliance with this policy and the secure handling of confidential information.

Approved by: The Heather Club Board of Trustees
Date: 17th January 2025

This Confidentiality Policy ensures that all staff, volunteers, and trustees of The Heather Club understand their responsibilities regarding the protection of personal and sensitive information and outlines the procedures for safeguarding confidentiality in line with legal and ethical standards.