Manager: Suzanne Campbell
Phone: 01796 539915

Abbey Place
Faversham
Kent ME13 7BG

Email: abbeyphysic@btinternet.com
Website: www.abbeyphysiccommunitygarden.org
Facebook: https://www.facebook.com/pages/Abbey-Physic-Community-Garden/119753674901502?fref=ts
Twitter: www.twitter.com/AbbeyPhysic

Abbey Physic Community Garden

Confidentiality Policy

Policy agreed	27 Mar 2010, May 2017, updated October 2022
Date of next review	October 2024
Signed: Agreed by Trustees October 2022	

Reasons for this Policy Statement

- To protect the interests of our members, staff, volunteers and other stakeholders
- To ensure all clients have trust and confidence in the Charity and that their dignity is respected
- To protect the Charity, its trustees, staff, members and volunteers
- To comply with data protection law

General principles

- Abbey Physic Community Garden (APCG) recognises that colleagues (employees, committee members, volunteers, trustees, and members) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from a manager.

- Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual.

- APCG recognises that there may be circumstance where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. However, colleagues are urged to share information with their line manager in order to discuss issues and seek advice in the first instance to avoid offending or upsetting other colleagues.

- Where there is a legal duty on APCG to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

Why information is held

- Most information held by APCG relates to members, employees, trustees, committee members, voluntary and community organisations, or services which support or fund them.

- Basic information on staff and members is kept to enable APCG managers and trustees to understand the experience, skills, background and history of the individuals in order to provide the most appropriate support and environment.

- Information on members' medications are kept to provide the necessary information to medical staff should an accident of emergency occur.

- APCG keeps information on funding sources and organisations and individuals that have provided services or support to the charity, or could in the future. This is in order to enable managers and trustees to identify potential funders and support.

- Information about ethnicity, religion/faith/belief, sexual orientation and disability of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

Access to information

- Information on members and staff is confidential to APCG Managers and Trustees.

- Information on supporters, services and funders used by APCG may be shared with community members requesting it, unless the organisation or individual has expressly told APCG that the information is confidential.

- Where information is sensitive, i.e. it involves disputes or legal issues, it will be confidential to the manager(s) dealing with the case and the trustees if necessary. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.

- Members may have sight of their personnel records by asking a manager.

- When photocopying or working on confidential documents, colleagues must ensure they are not seen by people in passing. This also applies to information on computer screens.

Storing information

- General non-confidential information about organisations is kept both in a lockable filing cabinet, accessible to managers, and when of interest to visitors of the garden and members, on a notice board or table in the pavilion.

- Members, staff, key holders, committee members and trustees' personnel information will be kept in lockable filing cabinets by managers or if digitally held, in secure password-protected folders.

- Confidential information should be labelled 'confidential' and kept in a lockable filing cabinet or held in digital password-protected folders.

- In an emergency situation, the manager or trustees may authorise access to this information by other people.

Duty to disclose information

- There is a legal duty to disclose some information including:

    - Child and vulnerable adult abuse or suspected abuse will be reported externally to the Social Services Department and follow our safeguarding procedures for sharing information, if appropriate.

    - Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.

- In addition, anyone believing an illegal act has taken place, or that a member is at risk of harming themselves or others, must report this to a manager who will report it to the appropriate authorities. We all have safeguarding responsibilities.

- Members should be informed of this disclosure.

Disclosures

- APCG follows GDPR guidelines and for DBS procedures regarding the correct handling, use, storage, retention and disposal of information.

- Disclosure information is kept in an applicant's personnel file in secure storage with access limited to those who are entitled to see it. It is a **criminal offence** to pass this information to anyone who is not entitled to receive it.

Data Protection Act

- Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles. These are that personal data must be:

    - Obtained and processed fairly and lawfully
    - Held only for specified purposes
    - Adequate, relevant and not excessive

- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with the Ac
- Kept secure and protected
- Not transferred out of Europe

We limit what information is stored on the computers. Personal and sensitive electronically stored information must be password protected.

Breach of confidentiality

Staff or volunteers should notify any potential breach, or risk of breach, to their line manager or a senior manager without delay; so that steps can be taken to remedy the situation.

- Members or staff who are dissatisfied with the conduct or actions of others at APCG should raise this with a manager using the complaints procedure, if necessary.

- Colleagues accessing unauthorised files or breaching confidentially may face disciplinary action. Ex-colleagues breaching confidentiality may face legal action.