Data Protection Policy

1. Introduction

This policy applies to the activities of the Hanover Community Association (HCA) including the management of the Hanover Centre. It applies to management committee members, paid staff and volunteers.

The purpose of this policy is to enable the HCA to:

- comply with the law in respect of the data it holds about individuals;
- follow good practice;
- protect HCA's supporters, staff and other individuals; and
- protect the organisation from the consequences of a breach of its responsibilities.

Personal data

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act.

Policy statement

HCA will:

- Comply with both the law and good practice.
- Respect individuals' rights.
- Be open and honest with individuals whose data is held.
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

HCA recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

- keeping information securely in the right hands; and
- holding good quality information.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, HCA will give individuals as much choice as is possible and reasonable about what data is held and how it is used.

Key risks

HCA has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out or shared inappropriately).
- Unauthorised sharing of information with other organisations.
- Insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed.
- Failure to offer choice about data use when appropriate.
- Breach of security by allowing unauthorised access.

- Harm to individuals if personal data is not up to date.

2. Responsibilities

The management committee recognises its overall responsibility for ensuring that HCA complies with its legal obligations.

The Chair of the management committee has particular responsibility for:

- Briefing the committee on Data Protection responsibilities.
- Reviewing Data Protection and related policies.
- Advising staff on Data Protection issues.
- Ensuring that Data Protection induction and training takes place.
- Notification (if required).
- Handling subject access requests.
- Approving unusual or controversial disclosures of personal data.
- Approving contracts with Data Processors.

The Chair may discharge the above responsibilities by supervising the actions of another committee member or employee.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work with the HCA.

Significant breaches of this policy will be handled under HCA's disciplinary procedures.

3. Confidentiality

Confidentiality applies to a much wider range of information than Data Protection, for example:

- Information about the organisation (and its plans, financial affairs, etc.).
- Information about other organisations, since Data Protection only applies to information about individuals.
- Information which is not recorded, either on paper or electronically.
- Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a "relevant filing system" in the Data Protection Act.

Information that falls within the scope of the Data Protection Act will always be handled in accordance with HCA's legal responsibilities.

Where a degree of confidentiality attaches to other information, access will normally be controlled on a strict 'need to know' basis. Where information poses a low risk (for example, lists of suppliers) control will be exercised on a proportionate basis.

HCA has adopted a privacy statement for Data Subjects setting out how their information will be used (see 'Privacy Statement' below below.) This is available on request, and a version of this statement is also available on the HCA web site.

Staff and volunteers will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities (see 'Confidentiality statement for staff and volunteers' below.)

Where anyone within HCA feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will

only be done with the authorisation of the Chair of the management committee. All such disclosures will be documented.

4. Security, data recording and storage

HCA has identified the following risks:

- Staff or volunteers with access to personal information could misuse it.
- Staff or volunteers could continue to be sent information after they have stopped working for HCA, if their records are not updated promptly.
- Poor web site security might give a means of access to information about individuals.
- Staff could feel an obligation to share information with partner organisations.
- Staff could be tricked into giving away information, either about supporters or colleagues, especially over the phone, through "social engineering".

Access to information on the main computer system will be controlled by function (for example, by password controlled user accounts).

HCA will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
- Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

HCA will establish retention periods for at least the following categories of data:

- Members.
- Supporters and users of services who elect not to become members.
- Volunteers.
- Staff.

Archived paper records and data backup files may be stored securely off site.

5. Subject Access

Any subject access requests must be referred to the Chair of the management committee who will oversee the handling of the request.

Where the individual making a subject access request is not personally known to the person dealing with them their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

HCA is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed;
- what types of disclosure are likely; and

- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Staff: in the staff handbook.
- Volunteers: in the volunteer support pack.
- Members: in the welcome pack.

6. Training

Information for management committee members is contained in the management committee handbook.

Information for staff is contained in the staff handbook.

All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.

Data Protection will be included in foundation training for volunteers.

7. Related Policies

Related policies include:

- Volunteer Policy

Date adopted:	March 2010
Last reviewed:	August 2014

Privacy Statement

The Hanover Community Association is committed to protecting your privacy. We will only use the information that we collect about you lawfully in accordance with the Data Protection Act.

We may collect information about you for a number of reasons, including:

- Entering into a room hire agreement with you,
- Enrolling you on a mailing list,
- Enrolling you as a volunteer or member, or
- Tracking how you use our web site.

By entering into these relationships with the HCA, you agree and accept that we may hold personal data about you and that we may contact you by virtue of the relationship we have established.

You may instruct us at any time to cease contacting you and we will do so immediately.

We will not share or disclose your personal information with any third party unless required to do so by law.

The type of information we will collect about you may include:

- your name
- address
- phone number
- email address

If you enter into a financial agreement with us, we may also collect:

- bank account details
- credit/debit card details

We will never collect sensitive information about you without your explicit consent.

We will delete financial information when the relevant transaction has been completed unless you grant us permission to retain the information.

The information we hold will be accurate and up to date. You can check the information that we hold about you by contacting us. If you find any inaccuracies we will delete or correct them promptly.

The personal information which we hold will be held securely in accordance with our internal security policy and the law.

We may use technology to track the patterns of behaviour of visitors to our web site. This can include using a "cookie" which would be stored by your browser. You can usually modify your browser to prevent this happening. Information collected in this way will only be used to improve the usability of the web site.

If you have any questions or comments about this statement, please contact us.

Confidentiality statement for staff and volunteers

When working or volunteering for HCA, you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are supporters or otherwise involved in the activities organised by HCA.
- Information about the internal business of HCA.
- Personal information about colleagues working for HCA.

HCA is committed to keeping this information confidential, in order to protect people and HCA itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by HCA to be made public.

You must also be particularly careful not to disclose confidential information to unauthorised people or organisations or cause a breach of security. In particular you must:

- **not compromise or try to bypass security measures** (including computer user account passwords);
- **not share the user account password** you use to log on to your computer with anyone who is not authorised to know it;
- **not allow anyone to use an HCA computer** unless their access has been approved by your manager or the HCA management committee;
- **not install any software** unless it has been approved by your manager or the HCA management committee;
- **log out** when you leave your computer to prevent unauthorised access;
- **lock the office door** behind you when you leave the room;
- **not gossip** about confidential information, either with colleagues or people outside HCA;
- **not disclose information** — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or allow access to information, do not guess. Withhold the information or access while you check with an appropriate person whether it is allowable.

Your confidentiality obligations continue to apply indefinitely after you have stopped working or volunteering for HCA.

I have read and understand the Data Protection Policy and the above statement.
I accept my responsibilities regarding confidentiality.

Signed: Date: