DATA PROTECTION POLICY

Approved by: Facilities and Finance sub-committee and Board of Directors
Lead Director(s): Debbie Abrams
Date of Approval: October 2017
Version: 3
Review Interval: three years
Review due by: October 2020
Appended Documents:
Responsibility for Dissemination and Implementation: CEO
Implementation date: October 2017

POLICY STATEMENT
The purpose of this policy is to enable BHCH to comply with its legal obligations in respect of the data it holds about individuals (both clinical and non-clinical), to follow good practice, to respect and protect patients, families, staff, volunteers and other individuals and to protect the organisation from the consequences of a breach of its responsibilities.

CONTENTS

Section		page
1	Introduction	1
2	Associated policies and procedures	2
3	Aims and objectives	2
4	Scope of the policy	3
5	Accountabilities and responsibilities	3
6	Method	3
6.1	Key Risks	3
6.2	Definitions	3
6.3	Staff responsibilities	5
6.4	Compliance with Statutory requirements	5
6.5	Confidentiality	5
6.6	Data recording and storage	6
6.7	Purposes for which personal data may be held	6
6.8	Sensitive personal data	6
6.9	Responsibility for the processing of personal data	7
6.10	Statement for written forms and web/email communications	7
6.11	Use of personal data	7
6.12	Personal data held for Equal Opportunities monitoring purposes	7
6.13	Procedure on disclosures	7
6.14	Accuracy of personal data and access to personal data	8
6.15	Procedure on subject access policy	9
6.16	Additional subject rights	9

6.17	GP / Medical report	9
6.18	Complaints and queries	10
6.19	Security	10
7	Equality impact assessment	10
8	Training requirements	11
9	Monitoring compliance with the policy	11
10	References	11
11	Policy Review	11
Appendix A	Privacy, Confidentiality and Security Statements	12
Appendix B	Data Protection Act Guidance	14

1. Introduction

Beaumond House Community Hospice recognises that its main priority under the Data Protection Act is to avoid causing harm to individuals. Information about patients, families, staff, volunteers and others must be kept securely, used fairly, and not disclosed/divulged to any person unlawfully or unnecessarily.

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

BHCH is the Data Controller and is registered under the Data Protection Act 1998 with the Office of the Information Commissioner. All processing of personal data will be undertaken in accordance with the data protection principles and to comply with the requirements of the Care Quality Commission, the regulatory body.

Policy and Procedure Drafting and Approval

Drafted with input from Finance and Facilities Board Sub-Committee and to be approved by the Board of Directors.

2. Associated Policies, Procedures and Guidance

- Confidentiality policy
- Human resources policies and procedures
- IT and email policy
- Information Governance Policy
- Patients Access to Health Records
- Procedures for health records creation, completion, storage and disposal

3. Aims and Objectives

BHCH will comply with the principles of the Act to ensure that information is:

- Processed fairly and lawfully and, shall not be processed unless specific conditions are met
- Obtained only for one or more of the purposes specified in the Act and shall not be processed in any manner incompatible with that purpose or those purposes
- Adequate, relevant and not excessive in relation to those purpose(s)
- Accurate and, where necessary, kept up to date
- Not kept for longer than is necessary
- Processed in accordance with the rights of data subjects under the Act

- Kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage, to personal information
- Ensure compliance with Caldicott Principles

Caldicott is specific to the NHS and organisations that provide NHS services and comprises six good practice principles, to which all staff must adhere. BHCH will adhere to the six principles:

- Justify the purpose(s) of using confidential information
- Only use confidential information if it is necessary
- If it is necessary, use only the minimum amount
- Access to information should be on a strict need-to-know basis
- Everyone must understand their role and responsibility
- Everyone must comply with and understand the law

4. Scope of the policy

All contracted and bank staff and volunteers who access information at BHCH

5. Accountabilities and Responsibilities

Everyone is accountable for personal compliance with this policy and the Leadership Team are responsible for ensuring staff and volunteers are aware of this policy and comply with its requirements.

6. Method

6.1 Key Risks

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

- Breach of confidentiality – information being given out inappropriately
- Insufficient clarity about the range of uses to which data will be put – leading to Data Subjects being insufficiently informed
- Data held is inaccurate or misleading
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access
- Failure to establish efficient systems – leading to personal data not being accurate or up to date
- Harm to individuals if personal data is not up to date
- Insufficient clarity about the way personal data is being used
- Failure to offer choices about use of contact details for patients, families, staff, volunteers and other individuals
- Failure to comply with legal requirements in processing, maintaining and securely storing personal data

6.2 Definitions

The Data Subject is the individual whose personal data is being processed and includes patients, families, carers, employees and volunteers (both current and past), job applicants, donors and suppliers.

Processing means the use made of personal data including:

- Obtaining and retrieving

- Holding and storing
- Making available within or outside BHCH
- Printing, sorting, matching, comparing, destroying

The Data Controller is the legal 'person', or organisation, that decides why and how personal data is to be processed. The Data Controller is responsible for complying with the Data Protection Act and is registered as such with the Office of the Information Commissioner. The Data Controllers for BHCH are: The Head of Care, The H R Manager and the Fundraising and Marketing Manager.

The Data Processor – BHCH is responsible for ensuring that all persons who process data have appropriate security and are aware of their responsibilities in undertaking the work. The responsibility of what is processed and how remains with the Data Controller.

The Data Protection Officer (DPO) is the name given to a person or persons within organisations who is the central point of contact for all data compliance issues. BHCH does not need an overall DPO because we are a small organisation. However, we do have named DPOs for specific areas of responsibility to help manage our processes effectively and ensure we are compliant with requirements. They will also ensure that any errors in personal data are corrected.

The named Data Protection Officers for the BHCH are:
- **Clinical** – Head of Clinical Services
- **Non-clinical** – HR Manager
- **Fundraising** – Fundraising and Marketing Manager
- **Financial** – Finance Manager

The Data Protection Officers are responsible for:
- Ensuring relevant information on data protection is made available to the Board of Directors
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection is covered during induction
- Handling subject access requests for their identified area of responsibility
- Approving unusual or controversial disclosures of personal data
- Electronic security
- Reporting any breaches to the CEO and onto the Information Commissioners Office following the process set out in the BHCH Near Misses, Incidents and Serious Incident Reporting Policy

The Fundraising Manager is responsible for approving data related statements on publicity materials and statements to the media generally.

Each member of staff and volunteer at BHCH who handles and/or processes personal data must comply with the organisation's operational procedures for handling personal data to ensure that good Data Protection practice is established and followed.

Confidentiality statements must be signed by all staff and volunteers however; volunteer data processors must sign the additional data protection letter.

Significant breaches of this policy may result in disciplinary action.

6.3 Staff Responsibilities

The Board of Directors recognises its overall responsibility for ensuring that BHCH complies with its legal obligations. This responsibility is devolved to the Chief Executive for operational purposes and, in turn, devolved by the Chief Executive to named individuals within the policy and/or members of the leadership team.

All staff are responsible for ensuring compliance with the policy. Inappropriate access to information retained on the computerised system may result in disciplinary action being taken.

6.4 Compliance with Statutory Requirements

The application of this policy complies with the following statutory requirements:

- Data Protection Act 1998
- Access to Health Records Act 1990 (about information held about patients who are deceased)
- Caldicott Committee Report

6.5 Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, BHCH has a separate Confidentiality Policy. All staff and volunteers sign the Hospice's Confidentiality Statement and are, therefore, acknowledging that they are aware of their duty of care in relation to confidential information.

6.6 Data recording and storage

BHCH has various databases holding information on patients, their families and carers, supporters and employees. Back-up files are produced daily and arrangements are in place for safe storage and retention. There is a separate policy about records management including how long records are kept for and when they are to be disposed of.

BHCH will regularly review its procedures for ensuring that records remain accurate and consistent and do not in any way contravene the principles of the Data Protection Act and ensuring:

- Databases are regularly reviewed to ensure accuracy and to facilitate the entry of accurate data
- Data on any individual will be held in as few places as necessary
- Databases will only be authorised and established by a senior manager
- Effective procedures are in place to ensure that systems and databases are updated when information changes
- Staff and volunteers who process detailed information about individuals will be updated on any changes in data protection
- Data will be immediately corrected if shown to be inaccurate

Archived personal data must be stored securely in locked cabinets and not generally accessible.

6.7 Purposes for which personal Data may be held

Personal data may be collected primarily for the purposes of:

- Patient referrals, discharges, auditing, data sets, government and other bodies
- Recruitment, promotion, training, redeployment and/or career development
- Administration and payment of wages and sick pay
- Calculation of certain benefits, including pension
- Disciplinary or performance management purposes
- Performance review
- Record of communication with employees and their representatives
- Compliance with legislation
- Provision of references to financial institutions, accessing educational development, to assist future/potential employers
- Staffing levels, succession and career planning
- Communicating with supporters of the charity, including members of the Lottery

BHCH considers the following personal data falls within the categories set out above:

- Personal details including name, address, age, status and qualifications.
- Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant
- References and CVs
- Emergency contact details
- Notes on discussion between line managers and employees
- IPRs and documents relating to grievance, discipline, promotion, demotion or termination of employment
- Training records
- Salary, benefits and bank/building society details
- Sickness and absence information
- For supporter records, details of donations are held in addition to name and address etc

Employees and applicants for employment with BHCH will be advised of the personal data which has been obtained and retained, its source and the purposes for which the personal data may be used or to whom it will be disclosed.

BHCH will review the nature of the information being collected and held on an annual basis to ensure there is a sound business reason for requiring the information to be retained.

6.8 Sensitive Personal Data

Sensitive personal data includes information relating to the following:

- Patient's medical information, treatment, care plan, etc.
- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual orientation
- Any offence – or alleged offence – caution, conviction, committed by the employee

6.9 Responsibility for the Processing of Personal Data

The BHCH Data Controller for BHCH is responsible for ensuring all personal data is controlled in compliance with the Data Protection Act 1998.

Employees who have access to and work with personal data must comply with this Policy and Procedure and adhere to the procedures laid down by the Data Controller. Senior/line managers must ensure that these members of staff have signed the Confidentiality Statement. Failure to comply with the Policy and Procedures may result in disciplinary action up to and including summary dismissal.

6.10 Statement for written forms and web/email communications

When data is collected the following statement must be included in all written forms and web/email communications:

'If you complete this form, BHCH will store and process your data in accordance with the requirements of its Data Protection Policy and in keeping with the Data Protection Act 1998'.

6.11 Use of Personal Data

In complying with the Data Protection Act 1998 and in the interests of privacy and confidentiality, BHCH will ensure employee confidence by using and disclosing information within the following guidelines:

- Personal data must only be used for one or more of the purposes specified within this policy
- Documents may only be used in accordance with the statement within each document stating its intended use (written or oral)
- Ensuring that identification of the individual employee is not disclosed when collecting or collating statistical information to respond to legitimate internal or external requests for data (patient analysis, surveys, data sets, etc)
- Personal data must not be disclosed, either within or outside the organisation, to any unauthorised recipient

6.12 Personal data held for Equal Opportunities Monitoring Purposes

Where personal data is obtained about patients, staff, candidates, for Equal Opportunities monitoring, all such data must be anonymised.

6.13 Procedure on Disclosures

BHCH will not allow data collected from subjects to be disclosed to third parties except in circumstances, which meet the requirements of the Data Protection Act. This will be either:

- The subject has consented to the disclosure.
- BHCH is legally obliged to disclose the data.
- There is a business requirement to disclose data that is within the remit of the Data Protection Act and is not prejudicial to the interests of the individual.

1. All employees must ensure any general disclosure is recorded on the `Table of Data' and each class of disclosure includes a clear rationale as to why this is taking place.

2. Any new disclosure to be made must be checked for suitability with the CEO. This may be referred to the Data Protection Registrar for advice.
3. Any request for data based on a legal requirement, e.g. from Police or other body, must be put in writing and be checked against the advice of the Data Protection Registrar before data is disclosed.
4. All employees and representatives have a duty to protect individual's data from accidental disclosure:
   * Do not give out passwords to other people, who will then have access to the data you are entitled to view.
   * Do not recycle reports that contain personal data.
   * Take due care to ensure that data is not left about on laptops or in files out of the office where they can be accessed by other people who are not BHCH employees or representatives.
5. In cases where sets of data are disclosed to non BHCH employees, for example external consultants carrying out specific reviews, employees must ensure that subjects have been informed of this use of their data, and why this is done. They must have had an opportunity to opt-out.

Where sensitive data is involved, employees or representatives should not disclose data to outside agents except in cases agreed by the CEO.

6.14 Accuracy of and Access to Personal Data

The organisation will review personal data regularly to ensure that it is accurate, relevant and up to date. All employees are reminded that they are required to notify any changes in personal data without delay, e.g. emergency contact, next of kin, change of name, address, telephone number, loss of driving licence where relevant, etc.

Employees have the right to access personal data held about them under section 4 of the Data Protection Act 1998 and 2003, e.g. computer or manual records. BHCH will provide information in response to any reasonable subject access request. BHCH will ensure data is kept in an accessible form to facilitate subject access.

There are, however, some limitations and exemptions to this right:

(i) Opinions given in confidence

Section 4(4A) allows for personal data containing expressions of opinion about the data subject that may be given to the data subject without the permission of the person who expressed that opinion but this does not include opinions 'given in confidence or on the understanding that it would be treated as confidential'.

An opinion given in confidence on the understanding that it will be kept confidential must satisfy a high threshold of confidentiality. By placing the word 'confidential' at the top of a page will not automatically render the data confidential. The Information Commissioner will look at the data and its context and will need to be satisfied that the data would not otherwise have been given but for this understanding. Managers will not normally be able to rely on the provision as it is an expected part of their role to give opinions on staff. Conversely, a colleague who reports a matter relating to an individual in confidence to a Senior/line manager could be expected to be protected by the confidentiality provision.

(ii) Professional legal privilege

The right of access does not apply to data in relation to communications between a client and his professional legal advisers

(iii) Protecting the source of data

Data does not have to be provided where revealing the source of the information would be to discourage others providing similar information in the future and would be contrary to the public interest, e.g. 'whistleblowing', reporting vulnerable adult or child abuse.

(iii) Investigation of an offence

If access would or could potentially prejudice a criminal investigation, it maybe refused.

(v) Other exemptions

Include: estimates of liability in respect of a compensation claim and back-up data

6.15 Procedure on Subject Access Policy

1. Employees and representatives will make every effort to ensure that immediate action is taken when a data access is requested.
2. A standard letter (amended as appropriate) will be sent to the subject stating BHCH's policy on subject access. This will promise to provide the required data to the best of BHCH's ability within 40 days. BHCH reserves the right to ask for a maximum payment of up to £10.
3. A search will be set up by the IT Officer to ensure that all relevant data will be collected and collated ready to present to the subject. The search will include all electronic data and ordered manual files if required. Information on data collection, storage, processing and transfer may be required.
4. The data will be offered to the subject at BHCH's premises with an employee on hand to help with any queries or interpretations. If the subject is unable to visit BHCH's premises, alternative arrangements can be negotiated.

6.16 Additional Subject Rights

The Consumer Credit Act 1974 and Data Protection Act 1998 provide certain specific rights to individuals. The BHCH Data Protection Policy recognizes these rights and will follow the requirements of the Act as required.

BHCH endeavours to ensure that all individual data is accurate. In the event of any inaccuracies being identified then steps will be taken to make appropriate corrections within a reasonable period. Additionally, if information provided to a third party is found to be inaccurate, then the third party will be contacted without delay to ensure that the inaccuracy is corrected.

6.17 GP/Medical Reports

Where a medical report is requested for a member of staff, the individual's agreement for 'access to medical reports' must be obtained, in writing. BHCH will ensure that a copy of that agreement must accompany the request letter to the individual's GP. The agreement must be very clear as to whether the member of staff requires 'sight of the medical report prior to disclosure to the employer'.

An employee has a right of access to medical data held by BHCH however, if there are grounds that the disclosure would be likely to cause serious harm to the physical or mental health of the data subject, it should not be made available.

Requests for access to personal data should be addressed to the respective Data Protection Officer:

Clinical – Head of Clinical Services
Non-Clinical – HR Manager
Fundraising – Fundraising and Marketing Manager

6.18 Complaints and Queries

- BHCH will respond to any complaints about data as quickly and responsively as possible. Any letter we receive in relation to the Data Protection Act, that questions our policy and/or procedure will be dealt within 5 working.
- Records will be kept of all correspondence for 6 years.

  The DPO handling the complaint or query will ensure they notify the CEO and that they continue to inform the CEO of any correspondence and developments as they occur.

6.19 Security

This section applies to security issues relating to personal data.

Access to information on the computer system is controlled by passwords and only those needing access are given the password. Staff and volunteers working on 'confidential' data must be very careful about information which is displayed on their computer screen and must make every effort to ensure that no unauthorised person can view the data when it is on display.

Any recorded information on patients, their families, staff and volunteers, donors and suppliers will be:

- **Stored in locked cabinets** – access is the responsibility of the line manager concerned and keys should be stored appropriately and not left in unlocked drawers
- **Protected using passwords** (if kept on computers) – passwords must comply with the IT Policy
- **Destroyed appropriately and confidentially if it is no longer needed** – it is recommended that personal data should be destroyed by the individual processing the information. If shredding is delayed for any reason the information must be retained under lock and key until it can be safely destroyed.

7. Equality Impact Assessment must be carried out on Policy and considered for all other documents

Equality Impact Assessment Tool

	Insert Name of Policy / Procedure	Yes/No	Comments
1	Does the policy / guidance affect one group less or more favourably than another based on:		
	· Race	No	
	· Ethnic Origin	No	
	· Nationality	No	
	· Gender	No	
	· Culture	No	

	· Religion or Belief	No	
	· Sexual orientation, including lesbian, gay or bisexual	No	
	· Age	No	
	· Disability - learning disabilities, physical disability, sensory impairment and mental health problems etc…	No	
2	Is there any evident that some groups are affected differently?	No	
3	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	N/A	
4	Is the impact of the policy/guidance likely to be negative?	No	
5	If so, can the impact be avoided?	N/A	
6	What alternatives are there to achieving the policy/guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	
	Name of Assessor (please print)		Signed
	Debbie Abrams		

8. Training Needs Analysis -Staff Training requirements

All staff dealing with records that fall within the remit of the Data Protection Act will have awareness/training on the requirements of the Act in relation to their work.

9. Monitoring Compliance with the policy / procedure.

Monitoring compliance will be by exception reporting of any breaches and auditing of responses to requests under the DPA.

10. References

Data Protection Act 2008
The General Data Protection Regulation (GDPR) set to take effect in the Spring of 2018

11. Policy Review

The policy will be reviewed every three years or sooner if legislation requires.

12 -Sign off sheet regarding dissemination of procedural documents

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Title of document:	**Complete and sign**
Lead Director:	
Sub Committee:	
Date Approved:	
Ratified by Board:	
Dissemination Lead:	
All relevant staff informed of changes, training plan in place to allow for full implantation.	
Date placed in policy files:	
Review Date:	

Appendix A

PRIVACY STATEMENT

When you request information from BHCH, sign up to any of our services or buy anything from us, BHCH obtains information about you. This statement explains how we process, store and maintain that information.

We have a legal duty under the Data Protection Act to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally, the information we hold comes directly from you. Whenever we collect information from you, we will make it clear which information is required to provide you with the information, service or goods you need. You do not have to provide us with any additional information unless you choose to. We store your information securely on our computer system, we restrict access to those who have a 'need to know' and ensure our staff know how to handle information securely.

We may have occasion to contact you regarding fundraising events, gift aid or other services which we provide and other ways in which you might like to support BHCH. You have the right to ask us not to contact you in this way. We will always endeavour to provide a clear method for you to opt out. You can also contact us at any time to ask us not to send you any future marketing material.

You have the right to request a copy of the information we hold about you – apart from information which may concern other people as well as you. Any such request must be made in writing to the Chief Executive at BHCH. There will be a charge to process and prepare this documentation. Failure to make requests in the correct way could result in a delay or your request not being processed at all.

STATEMENT OF CONFIDENTIALITY

All the information passing through this organisation is of a highly sensitive or confidential nature. It is therefore essential that any such information obtained by employees throughout the course of their duties, is not divulged to any persons outside the organisation. We provide a personal and professional service and it is imperative that a high standard is maintained in the discharge of responsibilities both to patients, families, other employees, volunteers, visitors, customers and members of the public. In accepting the confidence and trust of others we assume the obligation to keep knowledge of their health, private or business matters to ourselves.

You are therefore required either during the time you are working for Beaumond House or at any time thereafter, to keep confidential any personal, private or medical information relating to all persons as outlined above. This will include any confidential information belonging to the organisation of which you have gained knowledge throughout the course of your employment.

A breach of confidentiality may result in the need to invoke a formal process. You are expected to strictly adhere to these rules and in signing this statement, you have accepted that you will agree to abide by them.

STATEMENT OF SECURITY

BHCH cannot accept liability for loss or damage to personal property left on hospice premises during or outside your normal working hours even though reasonable precautions may have been taken.

You should be vigilant always and immediately report the presence of any suspicious persons or packages to your line manager/a senior manager and/or the Chief Executive.
It is the personal responsibility of all staff and volunteers to ensure every reasonable precaution is taken for the protection of Hospice property against damage, loss and theft.

DATA PROTECTION ACT 1998

During your work, you may meet information covered by the Data Protection Act 1998. In brief, this includes anything which is held on computer or in manual record form. Under the terms of the Act, information must be kept secure and may not be disclosed to unauthorised persons. The hospice is registered with the Office of the Information Commissioner.

In signing this statement, I understand and accept that I am bound by these conditions during and after my employment with BHCH.

Signed: …….

Please print name: …….

Date: ……..

Appendix B – Data Protection Act Guidance for Volunteers

Date

Name and Address

Dear

Re: Data Protection Act Guidance for Volunteers

As a volunteer working with BHCH you have already signed the Statement of Confidentiality and have agreed to abide by the principles of that Statement. However, as part of the duties you will be undertaking as a volunteer you will be encountering confidential and/or sensitive information relating to volunteers and/or patients. The information may include names and addresses or even information about people's circumstances, families, health, DBS information and other matters. To ensure that we exercise our duty of care to the Hospice, yourself, patients and other volunteers, we have set out below additional guidelines to support you during your volunteer duties. It is vital everyone understands what information they can and cannot access or share.

1. You must not divulge any hospice information or any information regarding individuals e.g. patients and/or volunteers to anyone.

2. You must ensure that you lock away any personal data relating to an individual when you leave the office or your workstation.

3. If you are working with personal data/information, it is for your eyes only and not to be shared with anyone else. You should not discuss any such information with anyone other than the department head with whom you are working.

4. Do not access any other personal details/information other than that which you have specifically been requested to work with.

5. If you are accessing/working with information on our databases, you must not use this for any unlawful reason and you must not copy information, which is the property of BHCH, in any format whatsoever.

6. If you are photocopying information please ensure you take it all with you and do not leave items on the copier or in the photocopier room.

7. You must not send personal data by email or copy personal data in any format whatsoever without the specific approval of the department head who you are responsible to.

8. You should not mention that any individual was at BHCH as the service user (patient) may not wish this to be known.

9 If you are asked for information whilst volunteering at BHCH, do not attempt to deal with the query but refer the enquiry to the department head with whom you are working. Please **do not** make an exception to this rule.

10. You are reminded that a breach of confidentiality is liable to result in your volunteering role being terminated.

If you are in any doubt whatsoever about what you may or may not do, please speak to either myself or the department head with whom you are volunteering.

I am enclosing a second copy of this letter, which I would ask you to sign and return to me confirming your acceptance of the above information.

Yours sincerely

Volunteer Co-ordinator

This is my formal acceptance of the above information, which I agree to abide by both during and after my volunteering duties with BHCH.

Signed: ……..…

Please print name: ……..

Date: ……..

Signed by the Volunteer Co-ordinator

Signed: …….....……..

Please print name: …….……

Date: ……..…