THE GATEHOUSE POLICY: Data Protection

Policy ID Number: P09
Policy Passed by Board of Trustees: July 2017 Valid until: July 2022

Introduction

1. The Data Protection Act 1998 (DPA) is a United Kingdom Act of Parliament which defines the law on the processing of data on identifiable living people and is the main piece of legislation that governs the data protection.

1.1. The purpose of this policy is to ensure that the Gatehouse complies with data protection principles when holding personal and sensitive information on staff, trustees, volunteers and Guests (users of the service).

Everyone within the organisation that is responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

1.2. The Gatehouse runs a drop-in café for the homeless and vulnerably housed six evenings a week. The organisation is volunteer led which is supported by a small staff team. There is designated Data Protection Trustee on the Board and annual Data Protection training will be delivered to staff and coordinators.

The type of data that we collect

2. The Gatehouse holds two types of data on individuals:

- Personal data e.g. includes a person's (a) name (b) date of birth (c) full address and postcode.
- Sensitive data e.g. ethnic origin, disability, risk and safeguarding.

Rights to access data held on you by the organisation

3. The Data Protection Act gives rights to individuals in respect of the personal data that organisations hold about them. If a person requests this information they will receive a copy within 14 working days of their request. If a person requests that the information held on them is destroyed, this will only be granted, if it is in accordance with the below timescales and regulations.

If there is a breach of data

4. There could be two types of data breach that the organisation could experience:

- If something has happened unintentionally, this should be reported to the Project Director as soon as possible. The organisation will report the breach to the Information Commissioners Office and review what we have learnt from the breach and implement changes (with the support of the designated Data Protection Trustee).
- An intentional breach will be if someone is deemed to be a risk to themselves or others (risk sharing protocol) or a safeguarding risk (safeguarding vulnerable adults). This policy should be read in conjunction with the Gatehouse Confidentiality policy and the Gatehouse Safeguarding Vulnerable Adults policy.

Who we keep data on and why

- The organisation holds information on Staff (paid workers), Volunteers (unpaid workers), Trustees (Board that governs the charity), Guests (users of the project), Job Applicants (unsuccessful candidates) and external organisations.
- This is to ensure that we comply with the Equality Act 2010, Employment Law, the organisations internal policies and liability insurance, to report to beneficiaries, commissioners and for day to day operational need.

6. How long we keep data for and why

A minimum of six years

- Volunteer information on an electronical database will be kept for a minimum of six years, due to the high turnover of volunteers and a large amount of volunteers returning. This is why we only take the minimum and actual personal information needed on volunteers. The information is purged every six years and the next date the database will be purged is April 2022.
- Staff HR files will be kept for a minimum of six years after employment has ceased for tax purposes. This will also include staff time sheets and rota.

A minimum of two years

- Unsuccessful job candidate's files will be kept for two years to evidence Employment Law and the Equality Act 2010 has been adhered to.
- Carry on Book files that hold a minimum of Guest information.
- One to One Project Worker Guest information.

A minimum of fifty years

- *Volunteer name under induction date in the annual office diary.
- *Staff name and employment start and end date (to be held by the Treasurer).
- *****Adult safeguarding incidents, complaints, grievances, disciplinary, redundancy, dismissal and Guest banning information.

***This is in case of an allegation of historical abuse which means the organisation needs to keep the relevant documents individuals information for a minimum of 50 years; this is part of a safeguarding management plan and to comply with the organisations liability insurance.**

How we securely destroy data

- Paper files will be shredded.
- Electronical files will be deleted from the server.

How we hold and manage data securely

7.The Gatehouse office space where most information is kept has two entrances. One entrance is secured (when not in use) by a lockable door and the other entrance is secured by three coded doors.

Type	Where	How	Who
Personal data	Mobile phones (iPhones)	1. Pin protected work mobiles, limited to 10 attempts before destruction. 2. Find My iPhone enabled for remote destruction. 3. Two-Step Authentication enabled to prevent unauthorised access to the Apple Account. 4. Personal numbers only given with consent.	Trustees Staff
	Office laptop	1. Windows account is password protected. 2. Kept in a locked office in a locked cabinet, when not in use.	Staff Internal computer technicians (x2)
	Mobile laptops	1. Laptop is Encrypted (when type of laptop allows). 2. Windows account is password protected. 3. Is put away out of sight when not in use.	Staff Trustees Internal computer technicians (x2)
	Internal volunteer database	1. Is password protected on a password protected laptop.	Staff
	Carry on Book	1. Is kept in a locked office.	Staff Coordinators
	Emails	1. Are password protected. 2. Logged out of when not in use 3. Two step authentication enabled.	Trustees Staff Internal computer technicians (x2)
	Food Safety folder (external volunteer information)	1. Is kept in a locked office.	Staff Coordinators
	Guest laptops	1. Are kept in a safe in a locked office when not in use. 2. Desk top message on all stating ‘all personal data will be deleted’. 3. Deletion of personal documents by computer technician (weekly).	Internal computer technicians (x2)
Sensitive data	Carry on Book	1. Is kept in a locked office.	Staff Coordinators
	Human Resources/ Safeguarding/ Complaints Cabinet	1. Is kept in a locked cabinet in a locked office.	Project Director
	One to One Worker Guest files	1. Is kept in a secure cabinet at home.	Staff
	Emails	1. Are password protected 2. Have Two-Step Authentication enabled. 3. Logged out of when not in use 4. Marked as ‘private & confidential’ when appropriate.	Trustees Staff Internal computer technicians (x2)