THE GATEHOUSE POLICY: General Data Protection Regulations (GDPR)

Policy ID Number: P10
Policy Passed by Board of Trustees: May 2018 Valid until: May 2023

Introduction

1. The purpose of this policy is to ensure that all the Gatehouse staff, volunteers and trustees are aware of how to comply with the GDPR which is the European wide law which will replace the current provisions under the existing Data Protection Act 1998. This law came into force in May 2018.

The main changes under GDPR

2. Many of the fundamental provisions of data protection in the current Data Protection Act 1998 are unchanged but the main changes are:

- Transparency- data subjects must be told why their data is being collected and how it is being used.
- Consent- if specific consent is required for use of certain data, this must be on an opt-in basis, not an opt-out one. Consent cannot be inferred from silence, pre-ticket boxes or inactivity and there must be simple ways for people to withdraw consent.
- Accountability- organisations must keep full records of their data holding and processing, together with the basis on which it is carried out.

The type of data collected

3. The Gatehouse holds two types of data on individuals:
3.1. Personal data e.g. can include a person's (a) name (b) date of birth (c) full address and postcode.
3.2. Sensitive data e.g. can include ethnic origin, disability, risk and safeguarding reporting.

Who has contact with data

4. The Gatehouse Treasurer, staff and coordinators are processors of data which can mean collecting, using, disclosing, retaining or disposing of personal/sensitive data.
4.1. The Gatehouse trustees are the data controllers. The data processors carry out the processing of data on behalf of the data controllers.

How to hold data

5. Data must be held in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**.**

5.1. Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data breach

6. A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The GDPR makes informing the ICO and the individuals affected compulsory in certain circumstances e.g. where there is a high risk to the individuals involved, for instance, through identity theft**.**

6.1. Some examples of a breach of data:

- Emails and attachments being sent to the wrong person/people
- Lost memory sticks which contain unencrypted personal data
- Malware- IT that does not have anti-virus software in place
- Unencrypted equipment theft
- Unencrypted loss of personal data
- CCTV- incorrect signage

6.2. If the Gatehouse experiences a breach of data under the new regulations, the following process will be implemented:

- The Project Director will inform and provide a written report to the Gatehouse GDPR trustee within 24 hours including details on how, when, what and the plan being put in place to address the breach.
- The Project Director will notify the Information Commissioner's Office within 72 hours with the above report.

6.3. The Gatehouse could be fined up to 4% of its annual turnover if there is a breach of data under the General Data Protection Regulations.

Why and how does the Gatehouse hold data?

7. The Gatehouse takes a person's privacy seriously and will only use your personal information for operational and lawful purpose. The Gatehouse will not sell your personal information on to any third party and information will be secured in a locked office (when not in use), locked cabinets and held on encrypted laptops.

The only time that information will be shared outside of the organisation with or without consent is when a person is deemed to be a risk to themselves or others or are obliged to do so by law.

Please see the Gatehouse data audit below that explains the data held, the reason why and for how long.

Guest Information/Data

Type of data	Where has it come from	Purpose of use	Who we share the data with	Length of time held	Security/Privacy measure
Personal & Sensitive Data	Drop in sessions. One to One Project Worker.	▪ Operational use. ▪ Safeguarding Vulnerable Adults. ▪ Risk management. ▪ Formal complaints. ▪ Grant applications and reporting (anonymised).	▪ Gatehouse Staff, Coordinators and Trustees. ▪ Appropriate professionals e.g. Adult Social Care and Local Authority. ▪ Grant awarding bodies (anonymously).	Sessional information in the Carry on Book & Banning notices= 2 years. Complaints, safeguarding reports, risk management reports = 50 years to comply with Safeguarding Vulnerable Adults Regulations and Liability Insurance. One to One Project Worker reports = 2 years after completion of work.	Paper files are secured in locked cabinets. Paper files are secured in the Project Directors locked cabinet and coded office. Blind copy email addresses to non-Gatehouse email addresses. Work laptops are encrypted. Windows account is password protected. Pin protected work mobiles, limited to 10 attempts before destruction. Find My iPhone enabled for remote destruction. Two-Step Authentication enabled to prevent unauthorised access to the Apple Accounts.

Donor Information/Data

Type of data	Where has it come from	Purpose of use	Who we share the data with	Length of time held	Security/Privacy measures
Personal & Sensitive Data	Donation of time e.g. volunteers. Donation of food e.g. food groups. Donation of funds e.g. individuals, groups, grants, sponsored events. Donations electronically, by post, by hand.	▪ Contact information for operational use. ▪ Safeguarding Vulnerable Adults e.g. front line volunteers, if applicable. ▪ Risk management e.g. front line volunteers, if applicable. ▪ Formal complaints e.g. front line volunteers & food groups, if applicable. ▪ Fundraising e.g. sponsored events on FaceBook & website (with consent).	▪ Gatehouse Staff, Coordinators and Trustees. ▪ Appropriate professionals e.g. Adult Social Care and Local Authority. ▪ FaceBook & website users.	Volunteer database = purged every 6 years due to high turnover. Food group database = immediate deletion of information once left. Name, induction dates, complaints, safeguarding reports, risk management reports = 50 years to comply with Safeguarding Vulnerable Adults Regulations and Liability Insurance. Grant applications and donors of funds = see appendix 1. Food group database = immediate deletion of information once left. Website & FaceBook= 6 months after completion of sponsored event.	Database is password protected on the office laptop which is encrypted and secured in locked cabinet. Paper files are secured in the Project Directors locked cabinet and coded office. Blind copy email addresses to non-Gatehouse email addresses. Windows account is password protected. Pin protected work mobiles, limited to 10 attempts before destruction. Find My iPhone enabled for remote destruction. Two-Step Authentication enabled to prevent unauthorized access to the Apple Accounts.

Staff Information/Data

Type of data	Where has it come from	Purpose of use	Who we share the data with	Length of time held	Security/Privacy measures
Personal & Sensitive Data	Paid staff.	▪ Retain employment history and compliance with Employment Law and the Equality Act 2010. ▪ Safeguarding Vulnerable Adults. ▪ Risk management. ▪ Formal complaints. ▪ Charities Act & Taxes Management Act. ▪ Equal Opportunity monitoring (anonymised).	▪ Treasurer and Project Director. ▪ Charity Commission. ▪ Pension, payroll and employee benefit providers, your employment lawyers (if applicable) and other professional advisers and HMRC.	Complaints, safeguarding reports, risk management reports = 50 years to comply with Safeguarding Vulnerable Adults Regulations and Liability Insurance. Unsuccessful recruitment applicants = 1 year. Staff files = 6 years after employment has ceased.	Paper files are secured in the Project Directors locked cabinet and coded office. Work laptops are encrypted. Blind copy email addresses to non-Gatehouse email addresses. Windows account is password protected. Pin protected work mobiles, limited to 10 attempts before destruction. Find My iPhone enabled for remote destruction. Two-Step Authentication enabled to prevent unauthorized access to the Apple Accounts.

Appendix 1 – Retention of Accounting Records and Other Related Documents

Document		Retention period	Reason for retention period
Cash Book*		Six years form end of financial year transaction made	Charities Act
Nominal Ledger*		-ditto-	-ditto
Sales Ledger*		-ditto	-ditto
Purchase Ledger*		-ditto	-ditto
Purchase Invoices		-ditto	-ditto
Petty cash records		-ditto	-ditto
Remittance advices		-ditto	-ditto
Correspondence re donations		-ditto	-ditto
Bank reconciliations		-ditto	-ditto
Gift Aid declarations		Six years after the last payment made	Data Protection Act
Legacies		Six years after the estate has been wound up	Data Protection Act
Income tax records for employees leaving		Six years plus current year	Taxes Management Act
Notice to employer of tax code		Six years plus current year	Taxes Management Act
Annual return of employees expenses – P11D (if any)		Six years plus current year	Taxes Management Act
Certificate of pay and tax deducted – P60		Six years plus current year	Taxes Management Act
Notice of tax code change		Six years plus current year	Taxes Management Act
Annual return of taxable pay and tax deducted		Six years plus current year	Taxes Management Act
Records of pension deductions		Six years plus current year	Pensions Act
Time sheets		Two years after audit	Audit
Payroll and payroll control account		Six years plus current year	Charities Act and Taxes Management Act
Accident books, accident records & reports		Three years after last entry or end of investigation if later	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
Personnel files & training records		Maximum six years after the employment ceased	Limitations Act 1980 & Data Protection Act 1998
Redundancy records		Six years	Data Protection Act
Application forms and interview notes (for unsuccessful candidates)		Six months to a year	Disability Discrimination Act 1995 and Race Relations Act 1976 recommend six months but one year limitation for defamation actions under Limitations Act

Note: * These records are maintained electronically on Quickbooks

Statutory Maternity Pay records		Three years after the end of the tax year in which maternity period ends	Statutory Maternity Pay Regulations
Statutory Sick Pay records		Three years after the end of the tax year	Statutory Sick Pay (General) Regulations
Insurance policies		Three years after lapse	Data Protect Act
Insurance claims correspondence		Three years after settlement	Data Protect Act

Employer's Liability insurance certificate		Forty years	Employer's Liability (Compulsory Insurance) Regulations 1998
Record of names of employees and volunteers with dates		Permanently	Requirement of insurance company in case of claims arising out of failure of safeguarding responsibilities
Trustee meeting minutes and resolutions		Minimum of ten years from date of the meeting	Charities Act
Annual Accounts & Trustee Report		Permanently	Data Protect Act