



# THE GATEHOUSE POLICY: General Data Protection Regulations (GDPR)

Policy ID Number: P10

Policy Passed by Board of Trustees: July 2018 Valid until: May 2021

## 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 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
<p style="writing-mode: vertical-rl; transform: rotate(180deg);"><b>Personal &amp; Sensitive Data</b></p>	<p>Drop in sessions.</p> <p>One to One Project Worker.</p>	<ul style="list-style-type: none"> <li>▪ Operational use.</li> <li>▪ Safeguarding Vulnerable Adults.</li> <li>▪ Risk management.</li> <li>▪ Formal complaints.</li> <li>▪ Grant applications and reporting (anonymised).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Gatehouse Staff, Coordinators and Trustees.</li> <li>▪ Appropriate professionals e.g. Adult Social Care and Local Authority.</li> <li>▪ Grant awarding bodies (anonymously).</li> </ul>	<p>Sessional information in the Carry on Book &amp; Banning notices= 2 years.</p> <p>Complaints, safeguarding reports, risk management reports = 50 years to comply with Safeguarding Vulnerable Adults Regulations and Liability Insurance.</p> <p>One to One Project Worker reports = 2 years after completion of work.</p>	<p>Paper files are secured in locked cabinets.</p> <p>Paper files are secured in the Project Directors locked cabinet and coded office.</p> <p>Blind copy email addresses to non-Gatehouse email addresses.</p> <p>Work laptops are encrypted.</p> <p>Windows account is password protected.</p> <p>Pin protected work mobiles, limited to 10 attempts before destruction.</p> <p>Find My iPhone enabled for remote destruction.</p> <p>Two-Step Authentication enabled to prevent unauthorised access to the Apple Accounts.</p>

# 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
<p style="writing-mode: vertical-rl; transform: rotate(180deg);"><b>Personal &amp; Sensitive Data</b></p>	<p>Donation of time e.g. volunteers.</p> <p>Donation of food e.g. food groups.</p> <p>Donation of funds e.g. individuals, groups, grants, sponsored events.</p> <p>Donations electronically, by post, by hand.</p>	<ul style="list-style-type: none"> <li>▪ Contact information for operational use.</li> <li>▪ Safeguarding Vulnerable Adults e.g. front line volunteers, if applicable.</li> <li>▪ Risk management e.g. front line volunteers, if applicable.</li> <li>▪ Formal complaints e.g. front line volunteers &amp; food groups, if applicable.</li> <li>▪ Fundraising/ Marketing e.g. sponsored events on FaceBook &amp; website (with consent).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Gatehouse Staff, Coordinators and Trustees.</li> <li>▪ Appropriate professionals e.g. Adult Social Care and Local Authority.</li> <li>▪ FaceBook &amp; website users.</li> </ul>	<p>Volunteer database = purged every 6 years due to high turnover.</p> <p>Food group database = immediate deletion of information once left.</p> <p>Name, induction dates, complaints, safeguarding reports, risk management reports = 50 years to comply with Safeguarding Vulnerable Adults Regulations and Liability Insurance.</p> <p>Grant applications and donors of funds = see appendix 1.</p> <p>Food group database = immediate deletion of information once left.</p> <p>Marketing= 6 months after completion of sponsored event.</p>	<p>Database is password protected on the office laptop which is encrypted and secured in locked cabinet.</p> <p>Paper files are secured in the Project Directors locked cabinet and coded office.</p> <p>Blind copy email addresses to non-Gatehouse email addresses.</p> <p>Windows account is password protected.</p> <p>Pin protected work mobiles, limited to 10 attempts before destruction.</p> <p>Find My iPhone enabled for remote destruction.</p> <p>Two-Step Authentication enabled to prevent unauthorized access to the Apple Accounts.</p>

# 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
<b>Personal &amp; Sensitive Data</b>	Paid staff.	<ul style="list-style-type: none"> <li>▪ Retain employment history and compliance with Employment Law and the Equality Act 2010.</li> <li>▪ Safeguarding Vulnerable Adults.</li> <li>▪ Risk management.</li> <li>▪ Formal complaints.</li> <li>▪ Charities Act &amp; Taxes Management Act.</li> <li>▪ Equal Opportunity monitoring (anonymised).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Treasurer and Project Director.</li> <li>▪ Charity Commission.</li> <li>▪ Pension, payroll and employee benefit providers, your employment lawyers (if applicable) and other professional advisers and HMRC.</li> </ul>	<p>Complaints, safeguarding reports, risk management reports = 50 years to comply with Safeguarding Vulnerable Adults Regulations and Liability Insurance.</p> <p>Unsuccessful recruitment applicants = 1 year.</p> <p>Staff files = 6 years after employment has ceased.</p>	<p>Paper files are secured in the Project Directors locked cabinet and coded office.</p> <p>Work laptops are encrypted.</p> <p>Blind copy email addresses to non-Gatehouse email addresses.</p> <p>Windows account is password protected.</p> <p>Pin protected work mobiles, limited to 10 attempts before destruction.</p> <p>Find My iPhone enabled for remote destruction.</p> <p>Two-Step Authentication enabled to prevent unauthorized access to the Apple Accounts.</p>

## 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

## Appendix 2 – Example of the Gatehouse Volunteer Starter Form

The Gatehouse use of volunteer data is in accordance with the General Data Protection Regulations (GDPR) 2018 and it will only be held for lawful and operational purposes. The Gatehouse will not sell volunteer data on to any third parties and it will be held and destroyed in a secure manner.

A Gatehouse volunteer has the right to ask for copies of all information held on them by the Gatehouse. Please request this information in writing to the Project Director [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive this within 30 days from the request date.

Under GDPR your data also has the *\*Right to be Forgotten* if the data held on you is not for a lawful purpose. Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive this within 30 days from the request date.

I consent to the below information to be held in a secure manner:

- **\*\*Name and induction date for a minimum of 50 years due to Safeguarding Vulnerable Adults Regulations.**
- **\*\*Personal details for a minimum of 50 years if I am involved in a safeguarding incident, complaint or allegation due to Safeguarding Vulnerable Adults Regulations.**
- **\*\*\*Details on this form for a maximum of 6 years for operational need.**

Please sign and tick the box if consent is given for all of the above:

Signature.....

Please complete the below in full:

Volunteer Personal Details:

I would like to become a Gatehouse volunteer. I am over eighteen and am happy to complete an introduction into the service. I have read the Gatehouse *policies and procedures on the website* and agree to abide by them.

Name:	Phone:
Date of birth:	Email:
Next of kin name:	Next of kin phone number:
Induction date:	

**WHILE THE GATEHOUSE HAS INSURANCE COVER AGAINST ACCIDENT AND INJURY TO ANYONE USING OUR PREMISES, AND EVERY CARE IS TAKEN TO ENSURE THEIR SAFETY, VOLUNTEERS SHOULD UNDERSTAND THAT THEY UNDERTAKE THIS WORK AT THEIR OWN RISK.**

I can confirm that I have read and understood the above:

Signature..... Date.....

\*The right to be forgotten means a right to request deletion of your data if not held for lawful purposes.

\*\*This is part of the Gatehouse safeguarding management plan and to comply with the organisations liability insurance.

\*\*\*The Gatehouse (front line) volunteer database will be purged every 6 years due to a high turnover of volunteers.



## Appendix 3 – Example of the Gatehouse Coordinator Induction Form

This checklist should be ticked, fully completed and signed for each new coordinator. A complete/signed copy should be kept in the Project Directors locked cabinet and also given to the coordinator.

1. Current coordinator identifies a new coordinator from current volunteer pool
2. An induction meeting is set up with the Project Director
3. Policies and procedures are given

### Coordinator Induction

1. Discuss all policies & procedures given
2. Discuss the coordinator role/responsibilities and handbook
3. Explain the importance of the organisations ethos and being Guest focus
4. Start date for coordinator training/shadowing booked

### General Data Protection Regulations 2018

The Gatehouse use of volunteer data is in accordance with the General Data Protection Regulations (GDPR) 2018 and will only be held for lawful and operational purposes. The Gatehouse will not sell volunteer data on to any third parties and will be held and destroyed in a secure manner.

A Gatehouse volunteer has the right to ask for copies of all information held on them by the Gatehouse. Please request this information in writing to the Project Director [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive this within 30 days from the request date

Under GDPR your data also has the *\*Right to be Forgotten* if the data held on you is not for a lawful purpose. Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive this within 30 days of the request date.

I consent to the below information to be held in a secure manner:

- Name and induction date for a minimum of 50 years due to Safeguarding Vulnerable Adults Regulations.
- Personal details for a minimum of 50 years if I am involved in a safeguarding incident, complaint or allegation due to Safeguarding Vulnerable Adults Regulations.
- Details on this form for a maximum of 6 years for operational need.

The Gatehouse would also like to email you with operational, marketing and fundraising materials that relate directly to the Gatehouse.

Please sign and tick the box if consent is given for all of the above:

Coordinator signature.....

### Induction completed

Project Director signature.....

Coordinator signature.....

Date.....

\*The right to be forgotten means a right to request deletion of your data if not held for lawful purposes.

## Appendix 4 – Example of the Gatehouse Staff Induction Form

### Staff Induction

1. Staff file compiled in a locked cabinet
2. All policies & procedures given:
3. Verbal introduction:
  - A history of the organisation
  - Ethos of the organisations
  - Discuss job description/expectations
  - Confirm hours of work
  - Staff meetings
  - Code of Conduct
  - Usual date of pay
  - Timesheets
  - Health & Safety
4. On the Job induction booked
5. First supervision booked

The Gatehouse use of staff data is in accordance with the General Data Protection Regulations (GDPR) 2018 and will only be held for lawful and operational purposes. The Gatehouse will not sell staff data on to any third parties and it will be held and destroyed in a secure manner.

A Gatehouse staff member also has the right to ask for copies of all information held on them by the Gatehouse. Please request this information in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive this within 30 days from the request date.

Under GDPR your data also has the *\*Right to be Forgotten* if the data held on you is not for a lawful purpose. Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive this within 30 days from the request date.

**I consent to the below information to be held in a secure manner:**

- Name, date of birth, start and end date to be held by the Treasurer for a minimum of 50 years due to Safeguarding Vulnerable Adults Regulations.
- Personal details for a minimum of 50 years if I am involved in a safeguarding incident, complaint or allegation due to Safeguarding Vulnerable Adults Regulations.
- My Human Resources file to be held for a maximum of 6 years after leave date for lawful purpose.

The Gatehouse would also like to email you with operational, marketing and fundraising materials that relate directly to the Gatehouse.

**Please sign and tick the box if consent is given for all of the above:**

Staff signature.....

### Induction completed

Project Director signature.....

Staff signature.....

Date.....

\*The right to be forgotten means a right to request deletion of your data if not held for lawful purposes.

## Appendix 5 – Example of the Gatehouse response letter to financial donors



Charity Registration No. 100 2741

### **THE GATEHOUSE**

St Giles Parish Rooms 10 Woodstock Road, Oxford. OX2 6HT

Phone: 01865 792999

Date

Dear (insert name)

I am writing to acknowledge and thank you for the kind donation of (insert amount) that you have made to the Gatehouse.

We very much appreciate your thoughts and support for the project and it goes a long way in helping the work that we do with the homeless and vulnerably housed in Oxford.

Yours sincerely,

The Gatehouse Team

The Gatehouse use of donor data is in accordance with the General Data Protection Regulations (GDPR) 2018 and will only be held for lawful purposes. The Gatehouse will not sell donor data on to any third party and will hold it in a secure manner. It will then be destroyed in line with GDPR. Please refer to the Gatehouse General Data Protection Regulations 2018 Policy on our website <http://oxfordgatehouse.org/> for more information.

## Appendix 6 – Example of the Gatehouse Marketing & Publicity Consent Form 2018

The Gatehouse use of data is in accordance with the General Data Protection Regulations (GDPR) 2018 and it will only be held for lawful and operational purposes. The Gatehouse will not sell data on to any third parties and it will be held and destroyed in a secure manner.

You have the right to ask for copies of all information held on you by the Gatehouse. Please request this information in writing to the Project Director [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive this within 30 days from the request date.

Under GDPR your data also has the *Right to be Forgotten*\* if the data held on you is not for a lawful purpose. Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) and you will receive a response within 30 days from the request date.

**I consent to the below information to be held in a secure manner for marketing and publicity purposes:**

- We may use your name, photograph and other personal data provided by you in the Gatehouse newsletters, on our website, or our social media accounts e.g. our Facebook or Twitter pages or other public communications media.\*\*
- We may keep your personal details on this form for a minimum of 2 for operational need e.g. contacting you to volunteer at publicity and raising awareness events.

Please tick this box if consent is given for all of the above:

Please also complete the boxes below in full:

	Your details:	If aged 13 or under your parent or guardian should also fill in their details below to confirm their consent:
Name		
Address		
Signature		
Date		

\*The right to be forgotten means a right to request deletion of your data if not held for lawful purposes.

\*\* Please note that requests to delete photographs and other personal data used in newsletters or other printed publicity material may result in the deletion of the original material, but not of any of the published documents themselves, including e-newsletters or downloadable versions made available online.

## Appendix 7 – Example of the Gatehouse website disclaimers

## Under Support/Donate Money

### Donors

The Gatehouse use of donors' data is in accordance with the General Data Protection Regulations (GDPR) 2018 and will only be held for lawful purposes. The Gatehouse will not sell donors data on to any third party and it will be held and destroyed in a secure manner once it is no longer require. Please refer to the Gatehouse General Data Protection Regulations 2018 Policy [here/link to policy](#) for more information.

If you would like to request a copy of the information that the Gatehouse holds on you (as a donor). Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) [link](#) and you will receive this within 30 days of the request date.

Under GDPR your data also has the *\*Right to be Forgotten* if the data held on you is not for a lawful purpose. Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) [link](#) and you will receive this within 30 days of the request date.

\*The right to be forgotten means a right to request deletion of your data if not held for lawful purposes.

### Fundraising

The Gatehouse use of fundraising data is in accordance with the General Data Protection Regulations (GDPR) 2018 and will only be held for lawful purposes. The Gatehouse will not sell donor data on to any third party and it will be held and destroyed in a secure manner once it is no longer required. Please refer to the Gatehouse General Data Protection Regulations 2018 Policy [here/link to policy](#) for more information.

If you are fundraising for the Gatehouse e.g. a sponsored event, we will only advertise your event details internally and externally e.g. the Gatehouse website and FaceBook page with your consent.

If you would like to request a copy of the information that the Gatehouse holds on you (as a donor). Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) [/link](#) and you will receive this within 30 days of the request date

Under GDPR your data also has the *\*Right to be Forgotten* if the data held on you is not for a lawful purpose. Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) [/link](#) and you will receive this within 30 days of the request date..

\*The right to be forgotten means a right to request deletion of your data if not held for lawful purposes.

## Under Volunteer/Information for Volunteers/Working at the Gatehouse &

### Under Volunteer/Information for Volunteers/Volunteer Groups Providing Food

The Gatehouse use of volunteer data is in accordance with the General Data Protection Regulations (GDPR) 2018 and it will only be held for lawful and operational purposes. The Gatehouse will not sell volunteer data on to any third parties and it will be held and destroyed in a secure manner. Once it is no longer required Please refer to the Gatehouse General Data Protection Regulations 2018 Policy [here/link to policy](#) for more information.

If you would like to request a copy of the information that the Gatehouse holds on you (as a volunteer). Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) [/link](#) and you will receive this within 30 days of the request date.

Under GDPR your data also has the *\*Right to be Forgotten* if the data held on you is not for a lawful purpose. Please put your request in writing to the Project Director at [katrina@oxfordgatehouse.org](mailto:katrina@oxfordgatehouse.org) [/link](#) and you will receive this within 30 days of the request date.

\*The right to be forgotten means a right to request deletion of your data if not held for lawful purposes.

Appendix 8 – Example of the Gatehouse privacy notice for Guests to be displayed in the project



Charity Registration No. 100 2741

**THE GATEHOUSE**

## PRIVACY NOTICE

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 held securely in a locked office (when not in use) and held on encrypted laptops.

The only time that information will be shared outside of the organisation is when a person is deemed to be a risk to themselves or others or we are obliged to by law. Consent will always have tried to be gained whilst the project is open unless it is deemed to be unsafe for you or others to do so.

Please ask a staff member for a copy of the Gatehouse Confidentiality Policy and General Data Protection Regulations Policy for more information on what type of information is held by the Gatehouse and for how long.