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

Policy ID Number: P09
Policy Passed by Board of Trustees: May 2023 - Valid until: May 2026

Introduction

A new domestic data privacy law called the United Kingdom General Data Protection Regulations (UK-GDPR) took effect on January 1st, 2021, and – alongside the Data Protection Act of 2018 and the Privacy and Electronic Communications Regulations (PECR) – governs all processing of personal data from individuals located inside the United Kingdom. The PECR sits alongside the data protection act and they give specific privacy rights in relation to electronic communications.

Personal data under the UK GDPR only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

The main points under the UK GDPR:

- The accommodation of domestic areas of data protection law.
- 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-ticked 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.
- An individual has the right to access personal data held on them.
- An individual has the right to request the correction and the updating the personal data held on them.
- An individual has the right to request to have your personal data erased.
- An individual has the right to object to the processing of their personal data or to restrict it for certain purposes only.
- An individual has the right to request data portability.
- An individual has the right to withdraw their consent to the processing at any time for any processing of data to which consent was obtained.
- It requires websites to obtain the explicit consent from users before processing their personal data via cookies and third-party trackers; it requires the need to safely store and document each valid consent; it requires a website to enable users to change their consent just as easily as they gave it; and it gives a set of rights to UK users, chief among them the right to delete and the right to have corrected already collected personal data.

Please see the Gatehouse Privacy Notice on https://oxfordgatehouse.org/privacy-notice/ for further details including how we manage data on the Gatehouse website.

The type of data collected at the Gatehouse

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, as an organisation is the data controller. The Gatehouse trustees, staff and volunteers are processors of data which can mean collecting, using, disclosing, retaining or disposing of personal/sensitive data.

4.1. Lamplight is a data processor for the Gatehouse and hosts and rectify system faults on the Gatehouse Management System. Please see the link on the Lamplight security procedures on https://www.lamplightdb.co.uk/the-system/gdpr/system-security/ and the Gatehouse privacy notice on https://oxfordgatehouse.org/privacy-notice/ for more information.

4.2. Krystal Hosting is a data processor for the Gatehouse and hosts the Gatehouse website. Please see the link on the Krystal Hosting privacy notice on https://krystal.uk/terms#privacy and the Gatehouse privacy notice on https://oxfordgatehouse.org/privacy-notice/ for more information.

4.3. A number of other third party organisations act as data controllers and/or data processors handling data related to purchases from, or donations to the Gatehouse or operating other fundraising schemes. See the Gatehouse privacy notice on https://oxfordgatehouse.org/privacy-notice/ for more information plus the privacy notices of these organisations as listed below. Please note that GDPR enquiries relating to these organisations should in the first instance be directed to them in line with their privacy notices and policies.

- Square is a payment processing provider on the Gatehouse website. Please see the Square privacy notice https://squareup.com/gb/en/legal/general/privacy
- GoCardless is a donations portal on the Gatehouse website. Please see the GoCardless privacy notice https://gocardless.com/privacy/payers/
- JustGiving is a donations portal on the Gatehouse website. Please see the JustGiving privacy notice https://www.justgiving.com/about/info/privacy-policy/privacy-policy-v30
- Charities Aid Foundation is a donations portal on the Gatehouse website. Please see the Charities Aid Foundation privacy notice https://www.cafonline.org/privacy
- Paypal Giving Fund is a donations portal on the Gatehouse website. Please see the Paypal privacy notice https://www.paypal.com/uk/legalhub/privacy-full
- American Express Membership Awards is a donations scheme on the Gatehouse website. Please see the American Express privacy notice https://www.americanexpress.com/en-gb/company/legal/privacy-centre/privacy-principles/
- Charitable Travel is a donations scheme on the Gatehouse website. Please see the Charitable Travel privacy notice https://www.charitabletravel.org/privacy-policy/
- British Airways Community Fund is a donations scheme on the Gatehouse website. Please see the British Airways privacy notice https://www.britishairways.com/en-gb/information/legal/privacy-policy
- Easyfundraising is a donations scheme on the Gatehouse website. Please see the Easyfundraising privacy notice https://www.easyfundraising.org.uk/privacy/
- Oxford Lottery is a fundraising lottery on the Gatehouse website. Please see the Oxford Lottery privacy notice https://www.oxfordlottery.org/privacy

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 EU. Unless you are processing or holding data transferred for the purposes of immigration control (or data which otherwise falls within the UK immigration exemption), data can still flow freely from the EEA because the EU have adopted adequacy decisions about the UK on the 28th June 2021.

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 UK 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 regulations, the following procedures will be implemented:

- The CEO will inform and provide a written report within 24 hours to the Gatehouse GDPR Trustee who is the Gatehouse Data Protection Officer. The report will include details on how, when and what the data breach is.
- The CEO will notify the Information Commissioner's Office within 72 hours to report the breach of data.
- The CEO will gain advice from the Information Commissioner's Officer on the actions/plan needed in relation to the data breach and implement the advice received.
- The CEO will provide a written report to the Gatehouse Data Protection Officer on completion of the data breach plan/advise received.
- The Gatehouse Operations Manager will follow and implement these procedures in the absence of the Gatehouse CEO.

6.3. The Gatehouse could be fined up to 4% of its annual turnover if there is a breach of data under the UK 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 purposes. The lawful bases under which they are held are primarily either legitimate interests (i.e. they are necessary to be able to carry out our operations), or legal obligation. In some cases, they are held for a specific purpose (e.g. publicity) based on having obtained prior consent.

The Gatehouse will not sell your personal information on to any third party and the only time that personal information will be shared outside of the organisation is when a person is deemed to be a risk to themselves/others, a safeguarding vulnerable adults concern or a child protection concern is raised, or when we are obliged to by law. Any such data held by us will be secured on encrypted hardware and software, in a locked office and cabinets (when not in use and/or data is kept in physical form) or on a secure cloud-based system/s within the UK.

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	Café/community centre. Delivery service Therapeutic, practical provision workshops. Casework service. Counselling service. The Women's Hub. The Lived Experience Advisory Forum. Professionals from external organisations.	▪ Operational use. ▪ Safeguarding Vulnerable Adults. ▪ Risk management. ▪ Formal complaints. ▪ Grant applications and reporting (anonymised). ▪ COVID-19 tracking purposes.	▪ Gatehouse Staff, Coordinators and Trustees. ▪ Appropriate professionals e.g. Adult Social Care and Local Authority. ▪ Grant awarding bodies (anonymously). ▪ Formal partner organisations. ▪ Lamplight (see section 4 information in this policy).	General Guest data across all service areas = 2 years after use of the service has ceased (except for see the below). . Complaints, safeguarding reports, risk management reports = 50 years to comply with Safeguarding Vulnerable Adults Regulations and Liability Insurance.	Paper files are secured in locked cabinets and locked in a door coded building. Non paper files are held on a secure cloud-based system within the UK. IT and Communications policy, procedures and disaster recovery plan are in place. Blind copy email addresses to non- Gatehouse email addresses. Work laptops are encrypted. Windows account are password protected. Two-Step Authentication enabled to prevent unauthorised access to the Apple Accounts. Pin protected and or/finger print protected work related mobiles. Limited to 10 attempts before destruction (IPhone). Guest names under work mobiles will be anonymised e.g. initials only.

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/ Marketing e.g. sponsored events on social media sites & website (with consent). ▪ COVID-19 tracking purposes.	▪ The relevant Gatehouse staff, coordinators and trustees. ▪ Appropriate professionals e.g. Adult Social Care and Local Authority. ▪ Social media & website users (with consent). ▪ Grant awarding bodies (anonymously). ▪ Square (see section 4 information in this policy). ▪ Krystal Hosting (see section 4 information in this policy). ▪ Lamplight (see section 4 information in this policy). ▪ Electronic donations portals and donation schemes (see section 4 information in this policy).	General volunteer/food donor data across all service areas = 2 years after volunteering has ceased (except for see the below). 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.	Paper files are secured in locked cabinets and locked in a door coded building. Non paper files are held on a secure cloud-based system/s within the UK. IT and Communications policy, procedures and disaster recovery plan are in place. Blind copy email addresses to non- Gatehouse email addresses. Work laptops are encrypted. Windows account are password protected. Two-Step Authentication enabled to prevent unauthorised access to the Apple Accounts. Pin protected and or/finger print protected work related mobiles. Limited to 10 attempts before destruction (IPhone). Guest names under work mobiles will be anonymised e.g. initials only.

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/employees. HM Revenue and Customs (HMRC).	▪ Retain employment history and compliance with Employment Law and the Equality Act 2010. ▪ Safeguarding Vulnerable Adults and children. ▪ Risk management. ▪ Formal complaints. ▪ Charities Act & Taxes Management Act. ▪ Equal Opportunity monitoring (anonymised). ▪ COVID-19 tracking purposes.	▪ Treasurer and CEO. ▪ 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 plus. current year of employment.	Paper files are secured in locked cabinets and locked in a door coded building. Non paper files are held on a secure cloud-based system/s within the UK. IT and Communications policy, procedures and disaster recovery plan are in place. Blind copy email addresses to non- Gatehouse email addresses. Work laptops are encrypted. Windows account are password protected. Two-Step Authentication enabled to prevent unauthorised access to the Apple Accounts. Pin protected and or/finger print protected work related mobiles. Limited to 10 attempts before destruction (IPhone). Guest names under work mobiles will be anonymised e.g. initials only

Appendix 1 – Retention of Accounting Records and Other Related Documents

Document		Retention period	Reason for retention period
Cash Book*		Six years from 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

Katrina Horne – Gatehouse CEO

Cathy Dolbear – Gatehouse Trustee

31st May 2023