



# BOWERS MILL

## APARTHOTEL

# GDPR AND DATA PROTECTION POLICY

BOWERS MILL HOTEL

2021

PREPARED BY POLICY PROS

# Contents

- Introduction.....3
- Scope .....4
- Definitions .....5
- Data Protection Principles – Clients and Staff .....7
  - Basis for Processing Personal Information – Clients and Staff.....7
  - Sensitive Personal Information – Clients and Staff.....8
  - Criminal Records Information – Staff.....10
  - Data Protection Impact Assessments (DPIAs) – Clients and Staff.....11
  - Documentation and Records - Staff.....12
  - Privacy Notice – Staff .....13
  - Individual Rights – Clients and Staff.....13
  - Individual Obligations - Staff.....14
  - Information Security .....15
  - Storage and Retention of Personal Information – Clients and Staff .....17
  - Data Breaches .....17
  - International Transfer of Data .....19
  - Staff Training.....19
  - Consequences of Failing to Comply .....19
- Data Storage and Retention .....20
  - Systems Used and Data Stored – Staff.....20
  - Systems Used and Data Stored – Clients .....20
  - Other Data Retention .....20
  - Sharing of Data .....21
  - Data Sharing Process Flow – Clients .....21
  - Client Data Stored.....23
  - Staff Data Stored.....24
- Subject Access Requests and Data Rights – Clients and Staff.....26
  - Introduction .....26
  - SAR and Data Rights Procedure .....26

SAR Timescales .....	26
SAR Fee's.....	26
SAR Business Processes .....	26
Undertaking Privacy Impact Assessments .....	27

## Introduction

Bowers Mill Hotel obtains, keeps, and uses personal information (also referred to as data) about clients, job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers, and apprentices for a number of specific lawful purposes.

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce and clients. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, and to being concise, clear, and transparent about how we obtain and use personal information relating to our workforce and clients, and how (and when) we delete that information once it is no longer required. The CEO, Company Directors and Senior Managers are responsible for informing and advising Bowers Mill Hotel and its staff on its data protection obligations, and for monitoring compliance with those obligations and with Bowers Mill Hotel's policies.

If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer Katie Duce:

- By Email: [katie.duce@bowersmillhotel.com](mailto:katie.duce@bowersmillhotel.com)
- By Letter: Bowers Mill Hotel, Branch Road, Barkisland, Halifax, West Yorkshire, HX4 0AD

## Scope

- This policy applies to the personal information of Clients, staff, former staff, temporary and agency workers, interns, volunteers, and apprentices.
- Staff should refer to the Bowers Mill Hotel Policy and, where appropriate, to its other relevant policies including in relation to data retention which contain further information regarding the protection of personal information in those contexts.
- We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update, or supplement it from time to time. We will circulate any new or modified policy to staff and any other stakeholders when it is adopted.

## Definitions

<b>Criminal Records Information</b>	Means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
<b>Data Breach</b>	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
<b>Data Subject</b>	Means the individual to whom the personal information relates;
<b>Personal Information</b>	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
<b>Processing Information</b>	Means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
<b>Pseudonymised</b>	Means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;

**Sensitive Personal Information** Sometimes known as ‘special categories of personal data’ or ‘sensitive personal data’ means personal information about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual’s health, sex life or sexual orientation.

**Controller** Art.2(d) GDPR

"Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws.

## Data Protection Principles – Clients and Staff

Bowers Mill Hotel will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner;
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- We will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- We will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

### Basis for Processing Personal Information – Clients and Staff

In relation to any processing activity, we will, before the processing starts for the first time, and then regularly while it continues

Review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing, for example:

- That the data subject has consented to the processing;
- That the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- That the processing is necessary for compliance with a legal obligation to which Bowers Mill Hotel is subject;
- That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or
- That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or



- That the processing is necessary for the purposes of legitimate interests of Bowers Mill Hotel or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.
- Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (for example, that there is no other reasonable way to achieve that purpose);
- Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
- Where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and
- Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether Bowers Mill Hotel’s legitimate interests are the most appropriate basis for lawful processing, we will:

- Conduct a legitimate interest’s assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
- If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
- Keep the LIA under review, and repeat it if circumstances change; and
- Include information about our legitimate interests in our relevant privacy notice(s).

#### Sensitive Personal Information – Clients and Staff

Sensitive personal information is sometimes referred to as ‘special categories of personal data’ or ‘sensitive personal data’.

Bowers Mill Hotel may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

- We have a lawful basis for doing so as set out above, for example, it is necessary for the performance of the employment contract, to comply with Bowers Mill Hotel’s legal obligations or for the purposes of Bowers Mill Hotel’s legitimate interests; and

- One of the special conditions for processing sensitive personal information applies, for example:
  - The data subject has given explicit consent;
  - The processing is necessary for the purposes of exercising the employment law rights or obligations of Bowers Mill Hotel or the data subject;
  - The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
  - Processing relates to personal data which are manifestly made public by the data subject;
  - The processing is necessary for the establishment, exercise or defence of legal claims; or
  - The processing is necessary for reasons of substantial public interest.
  
- Before processing any sensitive personal information, staff must inform a Bowers Mill Hotel Director of the proposed processing, in order that the data protection officer may assess whether the processing complies with the criteria noted above.
  
- Sensitive personal information will not be processed until:
  - The assessment/training has been agreed to; and
  - The individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
  
- Bowers Mill Hotel will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.
  
- Bowers Mill Hotel's Privacy Notice sets out the types of sensitive personal information that Bowers Mill Hotel processes, what it is used for and the lawful basis for the processing.
  
- In relation to sensitive personal information, Bowers Mill Hotel will comply with the procedures set out to make sure that it complies with the data protection principles set out above.
  
- During the recruitment process: the company will ensure that (except where the law permits otherwise):
  - During the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, for example: race or ethnic origin, trade union membership or health;

- If sensitive personal information is received, for example, the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;
- Any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;
- 'Right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;
- We will not ask health questions in connection with recruitment.
- During employment: the company will process:
  - Health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance, and facilitating employment-related health and sickness benefits;
  - Sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and
  - Trade union membership information for the purposes of staff administration and administering 'check off'.

#### Criminal Records Information – Staff

Bowers Mill Hotel are justified in obtaining criminal records information for a post if it is necessary:

- For the performance of the employment contract for that post.
- For the employer to comply with a legal obligation to which it is subject.
- To protect the vital interests of vulnerable service users; and
- For the purposes of the employer's legitimate interests.

Where a DBS check is identified as necessary, all application forms, job adverts, and recruitment briefs will contain a statement that an application for a DBS certificate will be submitted in the event of the individual being offered the position.

Applicants will only be asked to complete a criminal records information form before an offer of employment is made unconditional; they will not be asked to do so during the earlier short-listing, interview, or decision-making stages.

Criminal records information will be processed in accordance with the Bowers Mill Hotel DBS Policy.

#### Data Protection Impact Assessments (DPIAs) – Clients and Staff

Where processing is likely to result in a high risk to an individual's data protection rights we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate in relation to its purpose;
- The risks to individuals; and
- What measures can be put in place to address those risks and protect personal information.
- Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer in order that a DPIA can be carried out.
- During the course of any DPIA, the employer will seek the advice of the data protection officer and any other relevant stakeholders.

## Documentation and Records - Staff

We will keep records of processing activities, including:

- The name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);
- The purposes of the processing;
- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Where possible, retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- Information required for privacy notices;
- Records of consent;
- Controller-processor contracts;
- The location of personal information;
- DPIAs; and
- Records of data breaches.

If we process sensitive personal information or criminal records information, we will keep written records of:

- The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- The lawful basis for our processing; and
- Whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

- Carrying out information audits to find out what personal information Bowers Mill Hotel holds;
- Distributing questionnaires and talking to staff across Bowers Mill Hotel to get a more complete picture of our processing activities; and
- Reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

- We document our processing activities in electronic form so we can add, remove and amend information easily.

#### Privacy Notice – Staff

- Bowers Mill Hotel will issue privacy notices from time to time, informing staff about the personal information that we collect and hold relating to them, how they can expect their personal information to be used and for what purposes.
- We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

#### Individual Rights – Clients and Staff

Individuals have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed.
- To obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the SAR Policy information.
- To have data corrected if it is inaccurate or incomplete;
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as ‘the right to be forgotten’);
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim; and
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation’s legitimate grounds override your interests).

- If you wish to exercise any of the rights in paragraphs above, please contact the data protection officer.

#### Individual Obligations - Staff

- Individuals are responsible for helping Bowers Mill Hotel keep their personal information up to date. You should let Bowers Mill Hotel know if the information you have provided to Bowers Mill Hotel changes, for example if you move to a new house or change details of the bank or building society account to which you are paid.
- You may have access to the personal information of other members of staff, suppliers and clients of Bowers Mill Hotel in the course of your employment or engagement. If so, Bowers Mill Hotel expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out above.
- If you have access to personal information, you must:
  - Only access the personal information that you have authority to access, and only for authorised purposes;
  - Only allow other Company staff to access personal information if they have appropriate authorisation;
  - Only allow individuals who are not Company staff to access personal information if you have specific authority to do so from the data protection officer.
  - Keep personal information secure (for example, by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in Bowers Mill Hotel's Privacy Policy).
  - Not remove personal information, or devices containing personal information (or which can be used to access it), from Bowers Mill Hotel's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
  - Not store personal information on local drives or on personal devices that are used for work purposes.

- You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):
  - Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions being met;
  - Any data breach as set out below;
  - Access to personal information without the proper authorisation;
  - Personal information not kept or deleted securely;
  - Removal of personal information, or devices containing personal information (or which can be used to access it), from Bowers Mill Hotel's premises without appropriate security measures being in place;
  - Any other breach of this Policy or of any of the data protection principles set out above.

## Information Security

- Bowers Mill Hotel will use appropriate technical and organisational measures to keep personal information secure, and to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These may include:
  - Making sure that, where possible, personal information is pseudonymised or encrypted;
  - Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
  - A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
  
- In rare cases where Bowers Mill Hotel uses external organisations to process personal information on its behalf, additional security arrangements need to be



implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- The organisation may act only on the written instructions of Bowers Mill Hotel;
  - Those processing the data are subject to a duty of confidence;
  - Appropriate measures are taken to ensure the security of processing;
  - Sub-contractors are only engaged with the prior consent of Bowers Mill Hotel and under a written contract;
  - The organisation will assist Bowers Mill Hotel in providing subject access and allowing individuals to exercise their rights under the GDPR;
  - The organisation will assist Bowers Mill Hotel in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
  - The organisation will delete or return all personal information to Bowers Mill Hotel as requested at the end of the contract; and
  - The organisation will submit to audits and inspections, provide Bowers Mill Hotel with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Bowers Mill Hotel immediately if it is asked to do something infringing data protection law.
- Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the data protection officer.

## Storage and Retention of Personal Information – Clients and Staff

- Personal information (and sensitive personal information) will be kept securely in accordance with Bowers Mill Hotel's Information Security Policy.
- Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow Bowers Mill Hotel's Retention Policy which set out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the data protection officer.
- Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

## Data Breaches

A data breach may take many different forms, for example:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information either by a member of staff or third party;
- Loss of data resulting from an equipment or systems (including hardware and software) failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as a fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.

Bowers Mill Hotel will:

- Make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- Notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

## International Transfer of Data

Bowers Mill Hotel does not intend to transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein, and Norway) to other countries.

If this were to be required, it would be on the basis that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses.

## Staff Training

Bowers Mill Hotel will ensure that staff are adequately trained regarding their data protection responsibilities.

Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

## Consequences of Failing to Comply

Bowers Mill Hotel takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and Bowers Mill Hotel; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.

## Data Storage and Retention

Bowers Mill Hotel stores personal information on staff and some non-sensitive personal and business information and information on clients to fulfil their contractual obligations for room and service bookings at the hotel.

### Systems Used and Data Stored – Staff

- Paper documents on staff including applications, health checks and other personal information relevant to the employees' position are held securely in a locked file cabinet at the Hotel premises, with only authorised staff having access.
- Staff management data is held securely in cloud-based software Bright HR only accessible by supervisors for the purposes of scheduling and staff management including rotas and annual leave allocation.

### Systems Used and Data Stored – Clients

- Client information relevant to proof of identity and payment data is stored in Little Hotelier – a cloud based, secure Front Desk management system. Little Hotelier complies with double authentication defined in the Payment Services Directive (PSD2) and all EU GDPR directives.
- A client registration card containing personal information including nationality and car registration is printed and stored securely in a locked filing cabinet and then archive room.
- Various documentation that is produced throughout the client stay at the hotel may contain reference to the individuals(s). These include receipts, arrival/departure lists, invoices and so forth. These are all stored in a secure file cabinet – please refer to the Client Data stored table for more information.

### Other Data Retention

- CCTV is active at the premises, specifically in the public areas and is retained in an encrypted database with access only to authorised personnel.
- Google G Suite (also known as Google Workspace) is in use at the organisation and is used for document management and email for business related activities.

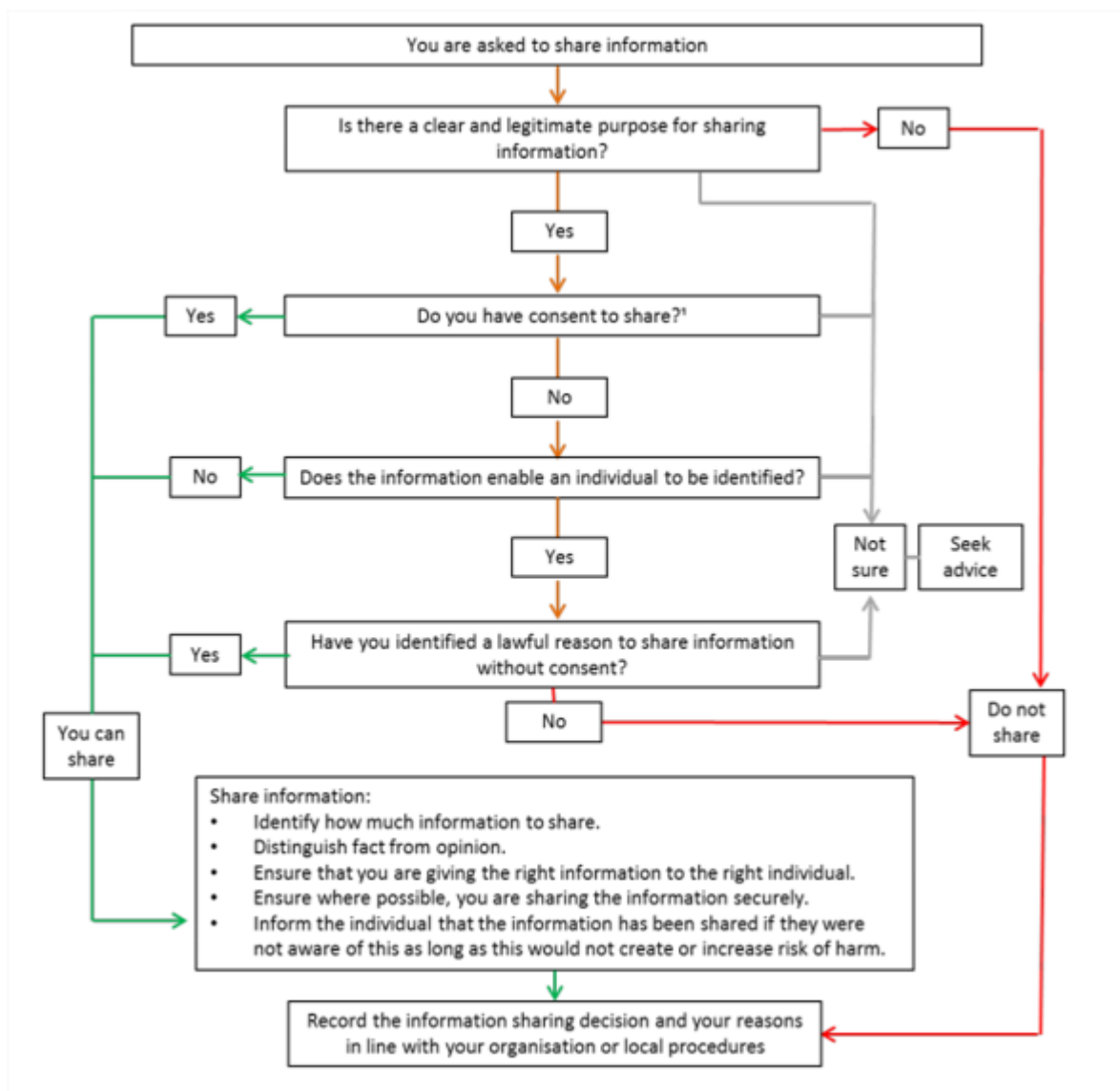
Access to all data is determined by the Hotel Manager and only staff with whose job remit requires it have access to personal or business sensitive information.

## Sharing of Data

Data is only shared when necessary with the following individuals and organisations:

- Payroll and Accounting services
- Local Authorities and Social Services (if required)
- Police and Government related organisations (if required)

### Data Sharing Process Flow – Clients





Client Data Stored

Information Type
Client Data
Data Stored
<ul style="list-style-type: none"><li>• Name</li><li>• Address</li><li>• Nationality</li><li>• Passport Number (if required)</li><li>• Police Warrant Cards (if required)</li><li>• Payment Card Details (encrypted through 3<sup>rd</sup> part provider for validation)</li><li>• Car Registration</li><li>• Room(s) booking data</li></ul> <p>Items that may contain client data:</p> <ul style="list-style-type: none"><li>• Deposit Reporting</li><li>• Room cleaning list</li><li>• Registration Card</li><li>• Accident Book Number</li><li>• Arrival/Departure lists</li><li>• Receipts and Invoices</li></ul>
Processing Reason
<ul style="list-style-type: none"><li>• Provision of Bowers Mill Hotel Services.</li></ul>



Legal Interest/Legitimate Reason
<ul style="list-style-type: none"> <li>• Legitimate reason for performing contract duties.</li> </ul>
Retention Policy
3 years from booking.

#### Staff Data Stored

Information Type
Staff Data
Data Stored
<p>The below bullet points show pieces of information that may be stored on staff members.</p> <p><b>Personal Information</b></p> <ul style="list-style-type: none"> <li>• Name, address, email, telephone number.</li> <li>• Next of Kin.</li> <li>• Application Form data/CV.</li> <li>• Interview notes.</li> </ul> <p><b>Contract</b></p> <ul style="list-style-type: none"> <li>• Dated/signed.</li> <li>• P60/P45.</li> </ul> <p><b>Photographic Evidence of Identity</b></p>

- Valid Passport/Driving Licence copy.

**Various**

- National Insurance and Bank details.
- Copies of relevant qualifications.
- Right to Work in the UK
- Evidence of Current Address (evidence to be no more than 6 months old at time of recruitment).
- References.
- Training Record.
- Record of sickness, leave and disciplinaries.

Processing Reason

- Provision of employment obligations.
- Fulfilment of contract.

Legal Interest/Legitimate Reason

- Legitimate reason for performing contract duties.
- Consent given by an individual at initial stage (contract).

Retention Policy

5 years after leaving service.

# Subject Access Requests and Data Rights – Clients and Staff

## Introduction

Under GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer their personal data, as well as object to automated decision-making based on their personal data.

## SAR and Data Rights Procedure

Subject Access Request should come to the email address [katie.duce@bowersmillhotel.com](mailto:katie.duce@bowersmillhotel.com) in the first instance and be followed up with an acknowledgement letter/email.

All requests and their progress must be logged by the data protection officer in a secure place with no external access.

## SAR Timescales

All Subject Access Requests will be completed within 30 days unless defined as complex – if the time will exceed 30 days, the requestor will be notified.

## SAR Fee's

Subject Access Requests coming directly from the data subject will be free, however Bowers Mill Hotel is able to charge a fee if requests become unfounded or excessive. If requests are coming from a Client on behalf of a data subject, Bowers Mill Hotel may charge a fee for data retrieval.

## SAR Business Processes

The processes cover SAR and other data rights of individuals:

- Right of Access and Data Portability
- Right to Erasure
- Right to Object
- Right to Restriction
- Right to Rectification

## Undertaking Privacy Impact Assessments

When Bowers Mill Hotel undertakes the use of new technologies or will be involved in the processing of data that contains a high risk to the rights and freedoms of data subjects, it will undertake a Privacy Impact Assessment.

The scale and nature of each PIA will be shaped on a case-by-case basis, with the objective of capturing the following information to inform the decision-making process:

- Risk Assessment
- Data types, collection, storage use and deletion methodologies
- Legal basis
- Information flows processes and procedures
- Consultation
- Evaluation of privacy procedures
- Final summary

For further information on PIA Please refer to:

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

Policy Date: February 2021

Review Date: February 2022

---

Dated and Signed by Director/Business Owner of Bowers Mill Hotel:

---