

# Data Protection (GDPR) Policy & Procedure

|                                                   |                                                   |
|---------------------------------------------------|---------------------------------------------------|
| <b>Updated by:</b> Celeste White – Office Manager | <b>Created:</b> January 2022 / updated July 2026  |
| <b>Director Sign Off:</b> Kay Brannon – Director  | <b>Version Control:</b> Update Required July 2027 |

DocuSigned by:  
  
98B04D53C87844E...

### Rationale:

Harrison Ince Ltd is committed to protecting the privacy and personal data of its employees, clients, suppliers, contractors and all other individuals whose information it processes.

The Company processes personal data in accordance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018**, and any other applicable data protection legislation.

As both a data controller and, where applicable, a data processor, Harrison Ince Ltd is committed to ensuring that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and kept up to date;
- retained only for as long as necessary;
- protected by appropriate technical and organisational security measures; and
- handled in accordance with the rights of individuals.

The Company processes personal data for legitimate business purposes including, but not limited to:

- recruitment, employment and payroll administration;
- delivering Architectural and Interior Design services;
- managing client, supplier and contractor relationships;
- maintaining records to meet contractual and legal obligations;
- invoicing and fee collection;
- complying with legal, regulatory and statutory requirements.

Harrison Ince Ltd is committed to ensuring that all personal data is collected, used, stored, retained and disposed of securely and lawfully.

### Compliance:

This policy applies to all employees, directors, contractors, agency workers, consultants and any third party who processes personal data on behalf of Harrison Ince Ltd.

All individuals covered by this policy must comply with the Company's Data Protection Policy, Privacy Notice, IT & Communications Policy, Social Media Policy and any related information security procedures when handling personal data.

Any breach of this policy or applicable data protection legislation may result in disciplinary action and, where appropriate, termination of employment or contractual arrangements.

Third parties with access to Company personal data will be expected to comply with this policy through appropriate contractual agreements.

This policy will be reviewed annually, or sooner where changes to legislation or business practices require it.

## UK General Data Protection Regulation (UK GDPR):

The UK General Data Protection Regulation (UK GDPR), together with the Data Protection Act 2018, sets out how organisations must collect, use, store and protect personal data.

Personal data means any information relating to an identified or identifiable living individual. This includes information held in both electronic and paper records, such as names, contact details, employment records, photographs, CCTV images and other information that can identify a person.

Individuals have a number of rights under UK GDPR, including the right to:

- be informed about how their personal data is used;
- access the personal data held about them;
- request correction of inaccurate or incomplete information;
- request the erasure of personal data where appropriate;
- restrict or object to certain types of processing;
- request the transfer of their personal data where applicable; and
- lodge a complaint with the Information Commissioner's Office (ICO).

Further information and guidance can be found on the Information Commissioner's Office website: [www.ico.org.uk](http://www.ico.org.uk)

## Data Retention and Disposal Requirements:

Harrison Ince Ltd retains personal and business information only for as long as necessary to fulfil the purpose for which it was collected, to meet legal, regulatory and contractual obligations, and to protect the Company's legitimate business interests.

Once the applicable retention period has expired, records will be securely destroyed or permanently deleted in accordance with the Company's data disposal procedures.

The standard retention periods are as follows:

| Record Type                                                           | Retention Period                                          |
|-----------------------------------------------------------------------|-----------------------------------------------------------|
| Customer personal data                                                | Duration of the customer relationship plus <b>6 years</b> |
| Employee personnel records                                            | Duration of employment plus <b>6 years</b>                |
| Employee contracts                                                    | <b>6 years</b> after employment ends                      |
| PAYE, tax and VAT records                                             | <b>7 years</b>                                            |
| Leave records                                                         | <b>3 years</b>                                            |
| Recruitment records (unsuccessful applicants)                         | <b>1 year</b> after interview                             |
| Planning records                                                      | <b>7 years</b>                                            |
| Health and Safety records (major accidents and dangerous occurrences) | <b>7 years</b>                                            |
| Public information                                                    | <b>3 years</b>                                            |
| Operational records                                                   | <b>5 years</b>                                            |

**Record Type**

Confidential business records

Critical financial records

**Retention Period**

**7 years**

**7 years**

Where legal proceedings, investigations or statutory requirements require information to be retained for longer than the periods stated above, records will be retained until the matter has been concluded.

**Data Protection Principles:**

Harrison Ince Ltd is committed to ensuring that all personal data is processed in accordance with the principles set out in the UK General Data Protection Regulation (UK GDPR). These principles underpin all activities involving the collection, use, storage and disposal of personal information.

**1. Lawfulness, Fairness and Transparency**

Personal data will only be processed where there is a lawful basis for doing so. Individuals will be provided with clear information about how their personal data is collected, used, stored and shared through the Company's Privacy Notice and other relevant communications.

**2. Purpose Limitation**

Personal data will be collected for specified, explicit and legitimate purposes and will not be used for any incompatible purpose unless permitted by law or where a further lawful basis applies.

**3. Data Minimisation**

Only personal data that is relevant, adequate and necessary for the intended purpose will be collected and processed. Harrison Ince Ltd will avoid collecting excessive or unnecessary information.

**4. Accuracy**

The Company will take reasonable steps to ensure that personal data remains accurate and up to date. Individuals are encouraged to notify the Company promptly of any changes to their personal information. Where inaccurate or incomplete information is identified, it will be corrected or deleted without undue delay.

**5. Storage Limitation**

Personal data will only be retained for as long as necessary to fulfil the purpose for which it was collected or to meet legal, regulatory or contractual requirements. Retention periods are detailed within the Company's **Data Retention and Disposal** section.

When personal data is no longer required, it will be securely destroyed or permanently deleted in accordance with the Company's data disposal procedures.

**6. Integrity and Confidentiality (Security)**

Appropriate technical and organisational measures will be implemented to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.

These measures include, where appropriate:

- restricting access to authorised personnel only;
- password-protecting systems and devices;
- encrypting personal data where appropriate;
- maintaining secure storage for both paper and electronic records;
- securely transferring personal information;
- securely disposing of confidential information when no longer required; and
- maintaining appropriate physical and cyber security controls.

All employees are responsible for protecting the personal data they handle and must immediately report any actual or suspected data breach to management in accordance with the Company's Data Breach Procedure.

## 7. Accountability

Harrison Ince Ltd is responsible for demonstrating compliance with UK GDPR. The Company will maintain appropriate policies, procedures, records and security measures to support compliance and will review these regularly to ensure they remain effective.

All employees are expected to comply with this policy and complete any data protection training required by the Company.

## Lawful Bases for Processing Personal Data:

Harrison Ince Ltd will only process personal data where there is a lawful basis to do so under the UK General Data Protection Regulation (UK GDPR).

Depending on the purpose of processing, the Company may rely on one or more of the following lawful bases:

- **Consent** – where an individual has given clear and informed permission for their personal data to be processed for a specific purpose.
- **Contract** – where processing is necessary to fulfil a contract with an individual or to take steps before entering into a contract.
- **Legal Obligation** – where processing is necessary to comply with legal or regulatory requirements.
- **Legitimate Interests** – where processing is necessary for the legitimate interests of the Company or a third party, provided those interests do not override the rights and freedoms of the individual.
- **Vital Interests** – where processing is necessary to protect someone's life.
- **Public Task** – where processing is necessary to perform a task carried out in the public interest or under official authority.

Where consent is relied upon, it must be freely given, specific, informed and unambiguous. Individuals have the right to withdraw their consent at any time, and doing so will not affect the lawfulness of processing carried out before consent was withdrawn.

Where another lawful basis applies, the Company will not rely on consent unnecessarily.

The lawful basis for processing personal data will be identified before personal data is collected or processed and will be recorded where required.

### **Subject Access Requests (SARs):**

Individuals have the right to request access to the personal data that Harrison Ince Ltd holds about them.

Any Subject Access Request (SAR) should be submitted to the Company's designated Data Protection Lead or other authorised representative. Any employee who receives a SAR must forward it promptly to the appropriate person for handling.

The Company will respond to a valid SAR without undue delay and, in most cases, within **one calendar month** of receiving the request. Where permitted by law, this period may be extended where requests are particularly complex or numerous, in which case the individual will be informed of the extension and the reasons for it.

The Company may request proof of identity before releasing personal information to ensure that data is disclosed only to the correct individual.

No fee will normally be charged for responding to a Subject Access Request. However, the Company reserves the right to charge a reasonable administrative fee or refuse a request where permitted by law, such as where a request is manifestly unfounded or excessive.

### **Disclosure and Sharing of Personal Data:**

Harrison Ince Ltd will only disclose personal data where there is a lawful basis to do so and where appropriate safeguards are in place.

Personal data may be shared where:

- the individual has given their consent, where consent is the appropriate lawful basis;
- disclosure is necessary to perform or fulfil a contract;
- disclosure is required to comply with a legal or regulatory obligation;
- disclosure is necessary to protect the vital interests of an individual;
- disclosure is necessary for the legitimate interests of the Company or a third party, provided those interests do not override the rights and freedoms of the individual; or
- disclosure is otherwise permitted or required by law.

Personal data will only be shared with authorised employees, trusted service providers or other third parties who have a legitimate business need to access the information and who are subject to appropriate confidentiality and data protection obligations.

Harrison Ince Ltd will never sell personal data or disclose it to unauthorised third parties.

Where personal data is shared with external organisations acting on behalf of the Company, appropriate contractual agreements and security measures will be in place to protect that information.

Employees must not disclose personal or confidential information unless they are authorised to do so and are satisfied that the disclosure complies with this policy and applicable data protection legislation.

### **Information Security:**

Harrison Ince Ltd is committed to protecting all personal, confidential and commercially sensitive information from unauthorised access, disclosure, alteration, loss or destruction.

The Company implements appropriate technical and organisational measures to ensure the security and confidentiality of the information it holds.

### **Access Controls**

Access to personal and confidential information is restricted to employees and authorised individuals who require it to carry out their duties.

All users are responsible for:

- keeping passwords secure and confidential;
- ensuring devices are password protected;
- locking computers and mobile devices when left unattended;
- preventing unauthorised access to Company information; and
- reporting any suspected unauthorised access immediately.

### **IT Security**

The Company maintains appropriate security measures including, where applicable:

- password-protected computers, laptops and mobile devices;
- firewall protection across Company systems and networks;
- anti-virus and anti-malware software;
- regular software and operating system security updates;
- secure cloud storage and encrypted data transfer where appropriate;
- regular data backups;
- appropriate access permissions; and
- secure disposal of electronic equipment and storage devices before disposal or reuse.

### **Physical Security**

Paper records containing personal or confidential information will be stored securely and access restricted to authorised personnel.

Confidential documents will be securely destroyed when no longer required in accordance with the Company's Data Retention and Disposal procedures.

### **Remote Working**

Employees who work remotely or access Company information outside the office must ensure that personal data remains secure at all times.

This includes:

- preventing unauthorised persons from viewing Company information;
- using only approved devices and systems where possible;
- securely storing paper records;
- avoiding the use of unsecured public Wi-Fi when accessing Company systems; and
- reporting any loss or theft of Company equipment immediately.

### **Data Breaches**

Any actual or suspected personal data breach, cyber security incident or loss of confidential information must be reported immediately to management.

The Company will investigate all reported incidents promptly and, where required, comply with its legal obligations for reporting personal data breaches to the Information Commissioner's Office (ICO) and affected individuals

### **Staff Responsibilities and training:**

All employees are responsible for protecting the personal data they process and for complying with this policy and all associated Company procedures.

Employees will receive data protection and information security awareness training as part of their induction and refresher training where appropriate.

Failure to comply with this policy or related information security procedures may result in disciplinary action in accordance with the Company's Disciplinary Policy.