DATA PROTECTION POLICY (GDPR)

MAIN POINTS

To help protect people's personal data keep to these Dos and Don'ts:

- Always treat people's personal information with integrity and confidentiality.
- Know what the data protection principles are and apply them.
- Store hard copies securely and transfer them directly to recipients.
- Use your encrypted USB drives to store and transfer data where needed.
- You have an organisational email address and remote access. Use it rather than send data to your personal email.
- Be alert to cyberattacks and report suspicious emails or calls.
- Report losses of data or devices as soon as possible.
- Take care to use the 'bcc' option for bulk emailing.
- Beware of autocomplete on email. Check you are sending to the right address.
- Ensure your personal device has appropriate security measures if using it for work-related activity.

1. INTRODUCTION

The security and management of data is important to ensure that we can function effectively and successfully for the benefit of our employees and clients.

In doing so, it is essential that people's privacy is protected through the lawful and appropriate use and handling of their personal information,

The use of all personal data by Hamilton Riley Limited is governed by:

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications Regulations (PECR)

Every member of staff has a responsibility to adhere to the Data Protection Principles outlined in the GDPR, and to this Data Protection Policy.

2. DATA PROTECTION PRINCIPLES

There are six Data Protection Principles defined in Article 5 of the GDPR. These require that all personal data be:

- Processed in a **lawful, fair** and **transparent** manner.
- Collected only for **specific, explicit** and **limited** purposes ('purpose limitation').
- **Adequate, relevant** and **not excessive** ('data minimisation').
- **Accurate** and kept **up-to-date** where necessary.
- Kept for **no longer than necessary** ('retention')
- Handled with appropriate **security** and **confidentiality.**

We are committed to upholding the Data Protection Principles. All personal data under our control must be processed in accordance with these principles,

3. LAWFUL PROCESSING

1. All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:

    - Where we have the **consent** of the data subject
    - Where it is in our **legitimate interests** and this is not overridden by the rights and freedoms of the data subject.
    - Where necessary to meet a **legal obligation**.
    - Where necessary to fulfil a **contract**, or pre-contractual obligations.
    - Where we are protecting someone's **vital interests**.
    - Where we are fulfilling a **public task**, or acting under official authority.

2. Any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR, must further be processed only in line with one of the conditions specified in Article 9(2).

3. The most appropriate lawful basis will be noted in the Data Processing Register. (See Section 5. Accountability).

4. Where processing is based on consent, the data subject has the option to easily withdraw their consent.

5. Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognised and adhered to by us.

4. DATA MINIMISATION AND CONTROL

1. Data collection processes will be regularly reviewed by the Data Governance Group to ensure that personal data collected and processed is kept to a minimum.

2. We will keep the personal data that we collect, use and share to the minimum amount required to be adequate for its purpose.

3. Where we do not have a legal obligation to retain some personal data, we will consider whether there is a business need to hold it.

4. We will retain personal data only for as long as it is necessary to meet its purpose. Our approach to retaining and erasing data no longer required will be specified in the retention policy and schedule. This schedule will be reviewed annually.

5. In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.

6. Anonymisation and pseudonymisation of personal data stored or transferred should be considered where doing so is a possibility.

5. ACCOUNTABILITY

1. Hamilton Riley Limited will maintain a Data Processing Register as required by Article 30 of the GDPR to document regular processing activities.

2. Hamilton Riley Limited have the responsibility of overseeing data protection and ensuring that we comply with the data protection principles and relevant legislation.

3. Hamilton Riley Limited will ensure that the Data Processing Register is kept up to date and demonstrates how the data protection principles are adhered to by our activities. Individual members of staff have a duty to contribute to ensure that the measures outlined in the Register are accurately reflected in our practice.

4. All employees, consultants or other parties who will be handling personal data on behalf of Hamilton Riley Limited will be appropriately trained and supervised where necessary.

5. The collection, storage, use and sharing of personal data will be regularly reviewed by Hamilton Riley Limited

6. We will adhere to relevant codes of conduct where they have been identified and discussed as appropriate.

7. Where there is likely to be a high risk to individuals rights and freedoms due to a processing activity, we will first undertake a Data Protection Impact Assessment (DPIA) and consult with the ICO prior to processing if necessary.

6. PROCEDURES FOR STAFF

While this policy helps us to demonstrate how we seek to comply with data protection legislation and be accountable for our actions.

All members of staff must comply with these procedures for processing or transmitting personal data.

- Always treat people's personal information with integrity and confidentiality. Don't hand out personal details just because someone asks you to.
- Where personal data exists as hard copy, it should be stored in a locked box, drawer or cabinet, and not left where anyone could access it.
- The transfer of hard copies should be passed directly to the recipient.
- Staff are issued with USB devices for the secure transfer of personal data or sensitive information.

7. RIGHTS OF DATA SUBJECTS

1. Under data protection laws, data subjects have certain rights:

- **Right to be informed.** The right to be told how their personal data is used in clear and transparent language.
- **Right of access.** The right to know and have access to the personal data we hold about them.
- **Right to data portability.** The right to receive their data in a common and machine-readable electronic format.
- **Right to be forgotten.** The right to have their personal data erased.
- **Right to rectification.** The right to have their personal data corrected where it is inaccurate or incomplete.
- **Right to object.** The right to complain and to object to processing.
- **Right to purpose limitation.** The right to limit the extent of the processing of their personal data.
- **Rights related to automated decision-making and profiling.** The right not to be subject to decisions without human involvement.

Julie Hamilton

JULIE HAMILTON
Director

01/06/2025