MARICE RECRUITMENT AGENCY LTD
EMPOWERING CARE, SUPPORTING OPERATIONS, ENSURING EXCELLENCE.

# Data Protection and Confidentiality Policy

## Policy Control Information

| Item | Details |
|---|---|
| **Policy Title** | Data Protection and Confidentiality Policy |
| **Policy Reference** | MRA-POL-010 |
| **Policy Owner** | MRA |
| **Designated Safeguarding Lead** | HR & DevOps |
| **Approved By** | Managing Director |
| **Issue Date** | 25/11/2026 |
| **Review Date** | Annually, and after any change in the law, a serious incident or an audit finding |

## 1. Policy Statement

Marice Recruitment Agency Ltd ("the company") handles a lot of personal data about candidates, workers, clients and staff, including identity documents, criminal record information and health details. The company protects that data, uses it only for clear and lawful reasons, and respects the confidentiality of everyone it works with, including the people its workers care for.

This policy is based on:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003
- Conduct of Employment Agencies and Employment Businesses Regulations 2003 (record keeping)
- Human Rights Act 1998, Article 8

## 2. Purpose

To make sure personal data is collected, used, shared, stored and deleted lawfully and securely, and that everyone knows what to do if something goes wrong.

## 3. Scope

This policy applies to all directors, managers and internal staff of Marice Recruitment Agency Ltd, wherever they are based, and to every worker the company supplies or introduces to clients in Healthcare Staffing, Warehouse, Logistics and Cleaning Services. It also applies to contractors,

suppliers and anyone acting on the company's behalf. It covers personal data in any form, on paper or electronic, including email, messaging apps and the company's systems.

## 4. Data Protection Principles

Personal data must be:

- Processed lawfully, fairly and openly
- Collected for clear, stated purposes and not used for anything else
- Adequate, relevant and limited to what is needed
- Accurate and kept up to date
- Kept no longer than necessary
- Kept secure

The company must be able to show that it follows these principles.

## 5. Special Category and Criminal Offence Data

Health information, information about ethnicity or other special category data, and DBS or other criminal record information are handled only where the law allows, seen only by staff who need them for safer recruitment or equality monitoring, and never shared more widely than needed. DBS certificate details are recorded (date, number, level and outcome), and copies are not kept unless there is a lawful reason.

## 6. Confidentiality Standards

- Information about clients, workers and the people at client sites is shared only on a need-to-know basis
- Workers must not discuss, photograph or post about the people they care for or the sites they work at, including on social media
- Candidate details are sent to a client only with the candidate's agreement for that client
- Staff must not use personal data from work for any personal purpose

## 7. Information Sharing

Personal data is shared with clients, payroll and pension providers, HMRC, the DBS and regulators only where there is a lawful basis and only what is needed. Data protection law does not prevent sharing information to protect someone from harm. Safeguarding information is shared in line with MRA-POL-006.

## 8. Data Security Measures

- Access to systems is by individual login, with multi-factor authentication where available, and passwords are never shared
- Access is limited to what each role needs
- Confidential files are kept outside public areas of the website and are shared through secure links rather than open attachments where possible
- Paper records are kept locked away and shredded when no longer needed
- Laptops and phones used for work are locked with a PIN or password
- Staff complete data protection training at induction and every year

## 9. Retention

Records are kept only as long as needed. Recruitment and assignment records are kept for at least one year after the company last provided services to the person or client, as the Conduct Regulations 2003 require. Payroll records are kept for at least three years after the end of the tax year. Right to work copies are kept during the engagement and for two years after it ends. The company's retention schedule sets out the period for each type of record.

## 10. Data Breach Procedure

1. Report any actual or suspected breach straight away to the DOQA Department Head.
2. Take steps to contain it, for example, recalling an email or disabling an account.
3. Record it in the breach log.
4. Assess the risk to the people affected.
5. Notify the Information Commissioner's Office within 72 hours of becoming aware of it, where it is likely to result in a risk to people's rights and freedoms.
6. Tell the people affected without delay where the risk to them is high.

## 11. Data Subject Rights

People have the right to be informed, to access their data, to have it corrected or erased, to restrict or object to its use, and to data portability. Requests can be made to info@maricerecruitment.co.uk and are answered within one month, extended only where the law allows.

## 12. Governance and Oversight

The DOQA Department Head and HR lead on data protection, keeps the breach log and the record of processing, makes sure the company's registration with the Information Commissioner's Office is kept up to date, and reports to the Managing Director, who has overall accountability.

## 13. Review

This policy is reviewed every year, and after a data breach or a change in data protection law.