Introduction

Malakoff needs to gather and use certain information about individuals, known as personal data. Personal data is any data that relates to a living individual who can be identified from that data.

The personal data collected by Malakoff can come from customers, suppliers, business contacts, employees and other people we have a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the requirements of the Data Protection Act and the General Data Protection Regulation (GDPR). The Data Protection Act and the GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children).

This Data Protection Policy ensures that Malakoff:

- Complies with the Data Protection Act and the GDPR and follows good practice.
- Protects the rights of employees, customers, suppliers and business contacts.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

The GDPR places a responsibility on Malakoff, as the Data Controller, to process any personal data in accordance the GDPR's six principles. These principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Policy Scope

This policy applies to:

- The head office of Malakoff.
- All branches of Malakoff.
- All staff and volunteers of Malakoff.
- All contractors, suppliers and other people working on behalf of Malakoff.

This policy applies to all personal and sensitive personal data that Malakoff holds both on computers/servers and in manual (paper based) files relating to identifiable individuals. This data can include:

- Names of individuals.
- Individuals' postal addresses.
- Individuals email addresses.
- Individuals telephone numbers.
- Individual's medical history.
- Individuals' gender.
- Any other personal data that may identify individuals.

Data Collection

If you are an employee or provide services to Malakoff, we will collect information in line with your contract of employment or contract for services.

If you have either purchased goods or services from Malakoff or act as a supplier to Malakoff, we only collect the basic personal data about you required to maintain our business relationship. This includes name, address, email, contact number(s) and banking information if you are an account holder.

Data Use

Personal data is of no value to Malakoff unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Therefore, all employees of Malakoff will comply with the below principles.

- When working with personal data, employees will ensure the screens of their computers are always locked when left unattended.
- Personal data will not be shared informally. In particular, it should never be sent by email as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data must never be transferred outside of the UK unless a risk assessment has been completed by the Malakoff HSQE Manager.
- Employees will not save copies of personal data to their own private computers.

Data Accuracy

- The law requires Malakoff to take reasonable steps to ensure data is kept accurate and up to date.
- It is the responsibility of all employees who work with personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible. For instance, by confirming a customer's details when they call or if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- Personal data will be held in as few places as necessary. Employees will not create any unnecessary additional data sets. This will allow the personal data to be kept as accurate as possible.
- Malakoff will make it easy for all data subjects to update the information Malakoff holds about them and how it is used.

Data Storage Security

These rules describe how and where data is safely stored. Questions about storing data safely can be directed to the Malakoff IT Administrator or the designated Malakoff Data Protection Officer (HSQE Manager).

When personal and sensitive personal data is stored on paper, it is kept in a secure cabinet where unauthorised people cannot see or access it. This also applies to data that is usually stored electronically but has been printed out for some reason.

The following principles will be followed by all Malakoff employees.

- When not required, the paper or files are kept in a locked drawer or filing cabinet.
- Employees will make sure paper and printouts are not left where unauthorised people could see them, like on a printer or unattended on desks.
- Personal or personal sensitive data printouts are to be shredded and disposed of securely when no longer required.

When personal or personal sensitive data is stored electronically,it is protected from unauthorised access, accidental deletion and malicious hacking attempts.

The below principles set out how this protection is achieved.

- Personal and personal sensitive data will be protected by strong passwords that are changed regularly and never shared between employees.
- If personal or personal sensitive data is stored on removable media (like an external drive), these will be kept locked away securely when not being used.
- Personal or personal sensitive data will only be stored on designated drives and servers.
- Servers containing data are sited in a secure location, away from the general office space.
- Data will be backed up daily, along with all other data on Malakoff's server.
- Personal or personal sensitive data is never to be saved directly onto private laptops or other private mobile devices like tablets or smart phones.
- All servers and Malakoff computers containing personal or personal sensitive data are protected by approved security software and a firewall.

Data Retention

The data retention period for employee's data can be found in the Employee's Privacy Notice that is issued to each employee.

The data retention period for external company's data that Malakoff hold can be found on the Customer Privacy Notice, which is available on the Malakoff website and upon request from the Malakoff Data Protection Officer (HSQE Manager).

Data Disclosure

The data disclosure information for employee's data can be found in the Employee's Privacy Notice that is issued to each employee.

The data disclosure information for external company's data that Malakoff hold can be found on the Customer Privacy Notice, which is available on the Malakoff website and upon request from the Malakoff Data Protection Officer (HSQE Manager).

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Malakoff will disclose the requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Electronic Data Back-Up

A back-up of the personal data, along with all the other data in the Malakoff's system, is taken as detailed in Malakoff Management Procedure P08 Document, Data, and Record Control.

Personal Data Security Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a controller or processor.
- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If a personal data breach occurs, Malakoff will ensure the following is carried out:

1. Containment and recovery of the personal data.
2. Assessment of ongoing risk.
3. Notification of breach.
   a. Individuals shall be informed directly and without undue delay about a breach if it is likely to result in a high risk to the rights and freedoms of the individuals. This can help them take steps to protect themselves from the effect of a breach.
   b. When a personal data breach has occurred, Malakoff need to establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, we must notify the ICO; if a risk is unlikely, we don't have to report it. However, if we decide we don't need to report the breach, we need to be able to justify this decision, so we shall document it. The report to the ICO must be made within 72 hours of discovering the breach.
4. All breaches shall be recorded. The record shall document the facts regarding the breach, its effects and the remedial action taken. Malakoff shall also investigate the cause of the breach and see how recurrence can be prevented.

Review of Policy

This policy will be reviewed every two years as a minimum, or when any new legislation or processes are introduced within the Company that affect this policy.

Signed By:  **Managing Director**

Date: 23rd May 2025 **Endorsed by Colin Duncan, Finance Director**

Issue 4