W R SWANN & CO LTD
DATA PROTECTION POLICY

Introduction:
W R Swann & Co Ltd needs to gather and use certain information about individuals.
These individuals can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.
This Policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Why this Policy exists:
This data protection Policy ensures that W R Swann & Co Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of employees, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law
The General Data Protection Regulation describes how organisations must collect, handle and store personal information.
These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

People, risks and responsibilities

Policy Scope:
This policy applies to:

- Swann-Morton Ltd, Swann-Morton (Services) Ltd, Swann-Morton (Microbiological Laboratory Services) Ltd, Jewel Blade Ltd and the W R Swann & Co Ltd Retirement Benefits Scheme
- All employees, job applicants, deferred pensioners, retired pensioners.
- All contractors, suppliers and other people working on behalf of the above companies.

It applies to all data that the group holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Data Protection Risks:
This policy helps to protect W R Swann & Co Ltd from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data

Responsibilities
Everyone who works for or with W R Swann & Co Ltd has some responsibility for ensuring data is collected, stored and handles appropriately.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

- The Board of Directors has ultimate responsibility for ensuring that we meet our legal obligations.

- The HR Manager is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies in line with an agreed schedule.
    - Arranging data protection training and advice.
    - Handling data protection questions.
    - Dealing with requests from individuals to see the data that we hold about them.
    - Checking and approving any contracts or agreements with third parties that may handle any of the company's sensitive data.
    - Approving any data statements attached to communications such as emails and letters.
    - Addressing any data protection queries from outside the company.
    - Where necessary, working with other employees to ensure marketing initiatives abide by data protection principles.

- The IT Department is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating third party services the company is considering using to store or process data. E.G. Cloud computing services.

General Staff Guidelines

- The only people able to access data covered by this policy are those that need it for their work.
- Data must not be shared informally. When access to confidential information is required, employees can request it from the HR Manager.

W. R. Swann & Co Ltd will provide training to all relevant employees to help them understand their responsibilities when handling data.

- Employees must keep all data secure by taking sensible precautions and following the guidelines below:
    1. In particular, strong passwords must be used and they must never be shared.
    2. Personal data must not be disclosed to unauthorised people, either within the company or externally.
    3. Data must be regularly reviewed and updated if it is found to be out of date. If no longer required, it shall be deleted and disposed of.
    4. Emails containing personal data must be deleted once read and acted upon.
    5. Employees shall request help from the HR Manager if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data must be safely stored. Questions about storing data safely can be directed to the HR Manager.

When data is stored on paper, it must be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files shall be kept in a locked drawer or filing cabinet.
- Employees must ensure that paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts must be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data must be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like CD or DVD), these shall be kept locked away securely when not being used.
- Data shall only be stored on designated drives and servers and if required, should only be uploaded to approved cloud computing services
- Servers containing personal data shall be sited in a secure location.
- Data shall be backed up frequently. The backups shall be tested regularly, in line with the company's standard backup procedures.

- Data shall never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data shall be protected by approved security software and a firewall.

Data Breach Escalation
In the case of a personal data breach, the company will without delay, and where feasible, not later than 72 hours after having becoming aware it, notify the personal data breach to the relevant supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.
This reporting of a personal data breach shall be performed by completing a Personal Data Breach Report form.

Data Use
It is usually when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.
- When working with personal data, employees must ensure the screens of their computers are always locked when left unattended.
- Particular care must be taken when sending personal data by email.
- Data must be encrypted before being transferred electronically. The IT Department can explain how to send data to authorised external contacts.
- Personal data will never be transferred outside of the European Economic Area.
- Employees shall not save copies of personal data to their own computers. Always access and update the central copy of any data.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data will be held in as few places as necessary. Staff shall not create any unnecessary additional data sets.
- Staff shall take every opportunity to ensure data is updated. For instance, by confirming an employee's details during a telephone conversation. Employee data will be updated regularly.
- Data shall be updated as inaccuracies are discovered. For instance, if an employee can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests
All individuals who are the subject of personal data held by W R Swann & Co Ltd are entitled to:
- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. All subject access requests must be referred to the HR Manager.
Subject access requests from individuals should be made in writing and the HR Manager will supply a standard request form.
The HR Manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, W R Swann & Co Ltd will disclose requested data. However, the HR Manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisors where necessary.

CCTV

The company uses CCTV recording equipment for security purposes around its premises. The company will display notices advising its employees and visitors, and members of the general public, that CCTV recording is in use. If requested by law enforcement agencies the company will provide them with CCTV footage. If a request is received from other legitimate agencies such as legal firms, the company will always verify their identity and assure itself that their request is legitimate and that consent has been obtained from the data subject, before disclosing any footage. If footage is disclosed, the company will ensure that the identity of any non-relevant data subject is protected.

Providing information

W R Swann & Co Ltd aims to ensure that individuals are aware their data is being processed and that they understand:

- How the data is being used.
- How to exercise their rights.

To these ends, the company has a privacy notice, setting out how data relating to individuals is used by the company.
All employees, and former employees or their families in receipt of pension from the W R Swann & Co Ltd Retirement Benefits Scheme, or former employees who are deferred members of the W R Swann & Co Ltd Retirement Benefits Scheme, will be made aware of the privacy statement and it will be provided to each employee on request. The full privacy statement is also available on the company's website and on company notice boards.