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

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 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 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.

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.

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.

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.