The Intern Group – data protection policy

CONTEXT AND OVERVIEW

Introduction

The Intern Group needs to gather and use certain information about individuals.

These 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 The Intern Group:

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

PEOPLE, RISKS AND RESPONSIBILITES

Policy scope

This policy applies to:

- The head office of The Intern Group
- All branches of The Intern Group
- All staff of The Intern Group

It applies to all data that the company 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 The Intern Group from some very real data security risks, including:

- Breaches of confidentiality - for instance, information being given out inappropriately.
- Reputational damage - for instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with The Intern Group has some responsibility for ensuring data is collected, stored and handled appropriately.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines in this policy.
- In particular, strong passwords must be used.
- Personal data should not be disclosed to unauthorised people.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

DATA STORAGE

These rules describe how and where data should be safely stored.

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

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

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- Data should only be stored on designated drivers and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.

DATA USE

Personal data is of no value to The Intern Group 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:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically.
- Employees should always access and update the central copy of any data.

PROVIDING INFORMATION

The Intern Group aims to ensure that individuals are aware that 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 statement, setting out how data relating to individuals is used by the company. This is available on request.