JAMES AND JAMES
eCOMMERCE FULFILMENT

Information Security Policy

Purpose & scope

This policy sets out James and James' ("the Company") process to ensure confidentiality, integrity and availability of data (electronically and in hardcopy) that it holds and processes.

The overriding objective is to protect the systems and data that the Company uses against any internal and external threats, in order to:

a. minimise the risk of damage to the data and systems used by the Company and

b. prevent unauthorised access or use of the data that belongs to the Company, its clients and staff.

This policy refers to all systems used to manage and run our business. This includes, but is not limited to: source code repositories, cloud infrastructure, tooling used for software development, corporate business systems (eg: email, drive, etc) and any third party applications relevant to the running of our business.

All users, employees or contractors and vendors, are responsible for adhering to this policy in all of their activities carried out on behalf of the Company.

Our employment policies set expectations of how we and everyone who works on our behalf will work to prevent Modern Slavery. All of our employees are provided with access to our policies upon joining the business, and they are required to complete a sign off on specific policies acknowledging that they have read and understood them.

Process steps

Data usage

Only uniquely identified, authenticated and authorised users must access and use data.

Data should be used only for the stated purpose of its collection or generation. In non-production environments data may be utilised for analysis, testing, and optimisation purposes. The data used will be limited to what is necessary for the continued support and development of our services and will remove personally identifiable information (PII) or sensitive data as appropriate.Any purpose outside the defined scope will be considered "misuse of data".

Each user must ensure that the Company's data under their control is properly labelled and safeguarded according to their sensitivity, proprietary nature, and criticality.

Access control mechanisms must also be utilised to ensure that only authorised users can access data to which they have been granted explicit access rights.

Data classification

All data in the processing environment must fall into one of the following categories:

- Confidential - only Leadership Team or specific, defined and required persons have access
- Restricted - designated employees have access
- Internal - all employees have default access
- Public information - everyone has access

To ensure the security and integrity of all data, the default classification for all data not classified by its owner must be Restricted.

Data storage

Data should only be stored for the time period necessary to fulfil its purpose, or to meet legal or regulatory requirements. Electronic data stored must be secured with encryption. Role Based Access Control (RBAC) mechanisms must be used to ensure only authorised users can access data to which they have been granted explicit access rights.

Data disposal

Stored or physical data assets must be disposed of in a secure manner such that it is completely destroyed and no information can be obtained from the waste.

Disposal of equipment

Equipment that may contain company or customer information must only be disposed of once it has been checked to ensure that all software and data has been completely removed from the item in question. Hard disk drives are to be removed wherever possible and rendered inoperable and then disposed of using a WEEE directive compliant supplier.

Disposal of documentation

Documentation that may contain confidential company or customer information must be shredded.

Transmitting data

A high degree of caution must be exercised when issuing information to external third parties. Confidential information should never be transmitted to external third parties without the prior approval of the Senior Leadership Team. Extreme care must be used in addressing data or messages to make sure that they are not sent to the wrong individual or company. In particular, exercise care using email.

Internet usage

The Company allows Internet access to its employees to facilitate communications with customers and others for business-related purposes.

Internet access must not be used to:

- Distribute or communicate confidential information, other than to customers, suppliers and other interested parties and only with their prior approval.
- Disseminate or print any copyrighted information in violation of copyright laws.
- Engage in any illegal activity.
- Download or distribute software without the prior written approval of a senior member of the Management Team.
- Engage in any activity that may cause network congestion or significantly hamper the ability of others to access and use the system.

Misuse of data

Any breach of this policy can have severe consequences to the Company, its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Intentional misuse of data resulting in a breach of any part of this policy will result in disciplinary action at the discretion of the Company's leadership and in accordance with people policy.

Severe, deliberate or repeated breaches of the policy by any employee may be considered grounds for instant dismissal, or in the case of a Company vendor, supplier or third party processor, termination of their contracted services.

User termination

When an individual leaves the employment of the Company their access rights shall be removed immediately, in accordance with 55.1.2 Leavers Process to ensure the security of the Company's systems.

Third party processors

Where James and James pass data to third parties for order fulfilment or address verification purposes, we validate that parties operate in accordance with our own Data Security Policy and accord our agreement with theirs. This includes, but is not limited to:

- **RoyalMail**
  https://www.royalmail.com/sites/royalmail.com/files/2023-08/General-Terms-and-Conditions-version-12.2.pdf
- **DHL**
  https://www.dhl.com/content/dam/downloads/g0/legal/summary_dpdhl_privacypolicy.pdf
- **DeutschePost**
  https://www.dhl.com/content/dam/downloads/g0/legal/summary_dpdhl_privacypolicy.pdf
- **Intersoft**
  https://intersoft.co.uk/privacy-policy-cookie-notice-intersoft/
- **SmartyStreets**
  https://www.smartystreets.com/legal/privacy-policy
- **EasyPost**
  https://www.easypost.com/privacy
- **Norsk**
  https://norsk.global/wp-content/uploads/2020/11/Norsk-Data-Protection-Policy-01-Ocober-2020.pdf

Portable information assets

Portable information assets and equipment can include, but is not limited to, laptops, mobile phones, digital cameras, any device that stores electronic data e.g. USB drives, hard drives

Under no circumstances should data be transmitted to removable media or taken from the Company's premises without the prior written approval from a senior member of the Management Team.

Transport and storage

Employees are responsible for ensuring the safe transport and storage of equipment belonging to the Company. They must not be stored in places where they can easily be stolen e.g. not left visible or unattended in a car or in overhead storage areas on a train.

Should any equipment be lost or stolen the users must immediately inform a member of the Management Team and update the asset tracking system.

Building access

Access to company premises shall only take place via authorised routes. An unauthorised person should be intercepted and brought to the attention of the Management Team.

Visitors

All visitors must report to reception, sign in and must be escorted at all times. Visitors must also sign out when leaving the premises.

Personal use of company IT equipment

Personal or non-business use of company issued equipment must not in any way inhibit or interfere with the performance of the employee or the systems or put the company's systems at risk.

Bring your own device (BYOD) and personal device management

All data stored or accessed on personal devices used for work purposes remains the exclusive property of the Company. Employees are granted the privilege to use personal devices for work-related tasks, but this does not transfer ownership or control of company data to the employee. The Company reserves the right to access, monitor, or delete any data on personal devices used for work purposes in order to protect its interests and ensure compliance with security protocols. Employees are responsible for implementing necessary security measures, such as password protection and encryption, to safeguard company data.

If employees use their own laptops/computers as part of their work duties:

- Use must be only when necessary and not in preference to a company issued device where one is made available
- Device must have up-to-date antivirus software installed, and recorded on the BYOD security software audit sheet
- Device must have a remote-wipe capability enabled
- Employee must avoid storing company data on local drive (use of Google Drive where possible is mandatory)
- Employee must ensure local drive in encrypted

Use of mobile devices for personal use

The company allows the use of personal devices such as mobile phones and tablets, but only with the prior approval of a member of the Management Team.

Access to Wi-Fi network

Access to the Company's Wi-Fi network shall require the approval of a member of the Management Team. Access is protected by password and WPA2/3 encryption.

Third-party data storage/analysis services

Management approval is required (and must be recorded in writing) before sharing company data with any third-party service, e.g. for process documentation, data formatting or analysis, etc.

Clear desk/screen

Computers and laptops must be protected with a screensaver during the working day when away from your desk i.e. screen locked. The maximum time before a user session is considered as idle must be configured at 15 minutes or below.

Confidential and sensitive information should be locked away when you are away from your desk, using the lockers provided, especially overnight.

Documents containing confidential and sensitive information must be removed from printers immediately. No documents should be left on printers overnight.

Privacy

By using the Company's systems and as a term and condition of employment, all system users acknowledge and consent to the Company's right to access, search, audit, intercept or review individual computer or network files, e-mail messages and Internet activity at any time with or without specific notice.

Availability

Copies of all company policies are available on Google Drive. Copies of the policy will be made available to interested third parties upon request.