DATA PROTECTION POLICY

ver. October 21, 2022

This Policy shall apply to collection, usage, and storage of personally identifiable information ("PII") by Index Franchising Limited, Index Property Information Limited, Index Insure Limited or any one of a combination of affiliated franchises businesses (collectively "Index"). Such PII may belong to customers, suppliers, business contacts, employees, or any other individual Index has a relationship with or may need to contact. This policy applies to Index head office, all Index branches, staff and volunteers, contractors, suppliers, and other people working on behalf of Index (collectively "Employees").

This Policy ensures that Index:

- Complies with applicable data protection laws and follows good practices
- Protects the rights of staff, customers, and partners
- Protects PII from inadvertent disclosure

Data Protection Law

This Policy is governed by the U.K. General Data Protection Regulation (UK GDPR) and The Data Protection Act 2018 (as amended) ("Privacy Laws"). The Privacy Laws apply regardless of whether PII is stored electronically, on paper or on other formats. PII must be:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Be processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

The PII may include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Personal information of third parties in connection with the products or services you request or order from us.
- Payment information (such as credit card and bank details)

This Policy helps to protect Index from:

- Inadvertent disclosure of PII

- Breaches of confidentiality
- Failing to offer choice i.e., all individuals should be free to choose how the company uses data relating to them
- Reputational damage

Responsibilities

Employees have a responsibility to ensure that the PII is collected, stored, and handled appropriately. Each team that handles PII will ensure that it is handled and processed in line with this Policy and Privacy Laws. Following individuals are appointed to ensure compliance with this Policy and Privacy Laws.

The Chief Compliance & Privacy Officer ("CCPO") is responsible for:

- Keeping the board updated about data protection responsibilities, risks, and issues
- Reviewing all data protection procedures and related policies
- Arranging data protection training for Employees
- Handling data protection questions from Employees
- Handling requests from data subject
- Reviewing and approving data protection agreements ("DPAs") with third parties that may handle Index's PII

The IT Manager 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 any third-party services Index is considering using to store or process PII

The Marketing team is responsible for:

- Coordinating with CCPO in approving any data protection statements attached to communications such as emails and letters
- Coordinating with CCPO in addressing any data protection queries from journalists or media outlets like newspapers
- Coordinating with CCPO to ensure marketing initiatives abide by Privacy Laws

General Staff Guidelines

- Employees will only be able to access PII on a need-to-know basis.
- PII will not be shared informally. The access can only be approved by line managers.
- Employees will be trained to help them understand their responsibilities when handling PII.
- Employees will keep all data secure, by taking precautions and following the herein below guidelines.
    - Strong passwords must be used and should not be shared
    - PII should not be disclosed to unauthorised people, either within Index or externally

- PII must be regularly reviewed and updated if it is found to be out of date
- PII must be deleted and disposed if no longer required
- Employees must request help from their line manager or CCPO if they are unsure about any aspect of data protection
- PII must not be sent via an email, as this form of communication is not secure
- Employees must ensure that the screens of their computers are always locked when left unattended while handling PII
- Data must be encrypted before being transferred electronically
- PII must not be transferred outside of the European Economic Area
- Employees must not save copies of PII on local drives
- PII must be protected by strong passwords
- If PII is stored on removable media, removable media must be kept locked away securely
- PII must be only stored on designated drives and servers
- PII must only be uploaded to approved cloud computing services
- Servers containing PII must be in a secure location, away from general office space
- PII must be backed up frequently. Those backups must be tested regularly, in line with Index's standard backup procedures
- PII must never be saved directly to laptops or other mobile devices like tablets or smart phones

Data Storage

These rules describe how and where data will be safely stored. Questions about storing data safely can be directed to the IT Manager. When data is stored on paper, it must be kept in a secure place where unauthorised people cannot access 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 should be kept in a locked drawer or filing cabinet
- Employees must ensure that paper and printouts are not left unattended on or near a printer
- PII printouts must be shredded and disposed of securely when no longer required
- When PII is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts
- All servers and computers containing PII must be protected by approved security software and a firewall.

Data Use

PII is of no value to Index unless the business can make use of it. PII is only collected when a customer:

- Registers to become a customer or user of our products or services
- Fills in and return to us a singed client form
- Uses our services by logging into our system or ordering products or services from us via our website, by phone, email or in other ways
- Enters PII into our system
- Stores details of products or services ordered

Data Accuracy

Privacy Laws require Index to take reasonable steps to ensure that PII is kept accurate and up to date.

- Duplication of PII should be avoided
- Employees must ensure that PII is always up to date
- Data subjects can reach out to request an update to the information held by Index
- PII should be updated to remove inaccuracies
- Marketing team must ensure that marketing databases are checked against industry suppression files every 6 months

Rights of Data Subjects

- Enquiring if Index hold any PII about them
- Reason for holding the PII
- Requesting a copy of PII help by Index
- Requesting an update to PII held by Index
- Requesting deletion of PII held by Index
- Requesting information regarding Index's compliance with Privacy Laws

Data Subject can send their requests at privacy.officer@dyedurham.com. Index will respond to such requests within a reasonable time. Index reserves the right to verify identity of a Data Subject making such a request to its satisfaction before handing over any information.

Disclosing Data for Other Reasons

Privacy Laws allows PII to be disclosed to law enforcement agencies without the consent of Data Subjects. Under these circumstances, Index will disclose requested data.

Providing Information

Index aims to ensure that individuals are aware that their PII is being processed, and that they understand:

- How the data is being used; and
- How to exercise their rights

Index Privacy Policy can be found at Privacy Policy
Index Cookie Policy can be found at Cookie Policy