



Introduction

Index Franchising Limited, Index Property Information Limited, Index Insure Limited or any one of a combination of affiliated franchises businesses (Index) 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 Index:

- 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 risks of a data breach

Data Protection Law

The Data Protection Act 1998 and the General Data Protection Regulation (GDPR) describe how organisations including the Companies 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.

The Data Protection Act and GDPR is underpinned by eight important principles. These say that personal data must:

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

Policy Scope

This policy applies to:

- The head office of Index
- All branches of Index
- All staff and volunteers of Index
- All contractors, suppliers and other people working on behalf of Index



It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 and GDPR. This can 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)

Data protection risks

This policy helps to protect Index from:

- **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 Index has some responsibility for ensuring data is collected, stored and handled appropriately.
Each team that handles personal data will ensure that it is handled and processed in line with this policy and data protection principles.
However, these people have key areas of responsibility:
 - The **board of directors of Index Franchising Limited** is ultimately responsible for ensuring that Index meet their legal obligations.
 - The **data protection officer, Anne Lucking**, 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 for the people covered by this policy.
 - Handling data protection questions from staff and anyone else covered by this policy.
 - Dealing with requests from individuals to see the data the Companies holds about them (also called 'subject access requests').
 - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
 - The **IT manager, Kevin Beck**, 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 the company is considering using to store or process data. For instance, cloud computing services.



- The **marketing manager, David Staple**, is responsible for:
 - Approving any data protection statements attached to communications such as emails and letters.
 - Addressing any data protection queries from journalists or media outlets like newspapers.
 - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **will not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- Index **provide training** to all employees to help them understand their responsibilities when handling data.
- Employees will keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords are used** and they are never be shared.
- Personal data **will not be disclosed** to unauthorised people, either within the company or externally.
- Data will 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.
- Employees **must request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

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 or data controller.

When data is **stored on paper**, it will 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 should be kept **in a locked drawer or filing cabinet**.
- Employees will make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts will be shredded** and disposed of securely when no longer required.
- When data is **stored electronically**, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data is **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these are kept locked away securely when not being used.
- Data is only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.



- Servers containing personal data are **sited in a secure location**, away from general office space.
- Data is **backed up frequently**. Those backups are tested regularly, in line with the company's standard backup procedures.
- Data will **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data are protected by **approved security software and a firewall**.

Data Use

Personal data is of no value to Index unless the business can make use of it. Personal information is collected by us when you:

- Apply to become a customer or user of our products or services.
- Fill in and return to us a signed client form.
- Use our services by logging into our system or ordering products or services from us via our website, by phone, email or in other ways.
- Enter personal information into our system about you or other persons in connection with your use or our products or services.
- Store details of products or services you have ordered or information and data contained in the particular products or services you have ordered.
- When working with personal data, employees ensure **the screens of their computers are always locked** when left unattended.
- Personal data **is not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data is **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data is **never transferred outside of the European Economic Area**.
- Employees **are not to save copies of personal data to their own computers**. Always access and update the central copy of any data.

Data Accuracy

The law requires Index to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Index should put into ensuring its accuracy.

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 is held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.
- Index make it **easy for data subjects to update the information** Index hold about them. For instance, via the company website.



- Data is be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject Access Requests

All individuals who are the subject of personal data held by Index 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.

Subject access requests from individuals should be made by email, addressed to the data controller at data.controller@indexpi.co.uk. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller 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 Data Protection Act and GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Index will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing Information

Index 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. A version of this statement is also available on the company's website.

Signed as confirmation that I will as far as I am able ensure the terms of this policy are adhered in full by myself and my employees.