Data Protection Policy

Key Details

- Policy prepared by Impact Express
- Approved by board/management on Impact Express
- Policy became operational on 01/05/18
- Next review date 23/05/19

Introduction

Impact Express 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 Impact Express:

- Complies with data protection law and follow 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 data breach
-

Data Protection Law

The Data Protection Act 1998 describes how organisations – including Impact Express 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 is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and unlawfully
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. 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

People, Risks and Responsibilities

Policy scope

This policy applied to:

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

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. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Credit/Debit card details
- Telephone numbers
- Information provided when filling in online forms via our website
- And any other information relating to individuals

Data Protection Risks

This policy helps to protect Impact Express 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.

Responsibilities

Everyone who works for or with Impact Express has some responsibility for ensuring data is collected, stored and handled 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, these people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that Impact Express meets its legal obligations.
- The Data Protection Officer, Andrew Kempster, is responsible for:
    - Keeping the board updated about data protection responsibilities, risk 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.
    - Dealing with requests from individuals to see the data Impact Express holds about them (also called 'subject to access requests')
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The IT Manager, Kelly Miller, 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, Amrita Daggar, is responsible for:
    - Approving 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 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 should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Impact Express will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it's found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection offer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should 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 should 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 should make sure proper and printouts are nit left where unauthorised people could see them, like a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

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.
- If data is stored on removable media (like CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- 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.
- Data should never be saved directly to laptop or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is if no value to Impact Express 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. In a particular, it should never be sent by email, as this is a form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send date to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

When you consent/ opt in in to the Impact Express mailing list, we will send you marketing communications and news concerning Impact Express' services, events and promotions. You can opt-out at any time after you have given your consent.

Data Accuracy

The law requires Impact Express 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 Impact Express should put into ensuring its accuracy.

It is the responsibility of all employees' who work with the data, take responsible 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 should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming customers details when they call.
- Impact Express will make it easy for data subjects to update the information Impact Express holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their telephone number, it should be removed from the database. It is the marketing managers responsibility to ensure marketing database are checked against industry suppression files every six months

Subject Access Requests and Right of Access

All individuals who are the subject of personal data held by Impact Express are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Customers/clients passwords will not be accessible to Impact Express employees
- Customers/clients have the right to change their passwords at any time
- Customers/ clients have the right to opt in to our mail list
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations.

If an individual contracts the company requesting the information, this is called a subject access request.

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

Right to Be Forgotten and Deleting of Data

The right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data and potentially have third parties halt processing of data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for process, or data subjects withdraw consent. It should also be noted that this right requires controllers to compare the subjects right to "the public interest in the availability of the data" when considering such requests.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

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

Providing Information

Impact Express aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How is the data 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.

If you are not satisfied with how we handle your information, or would like to complain you can exercise your rights please contact Impact Express at office@imapactexpress.co.uk.

If you are not satisfied with our response to your complaint, you can extend your complaint to the UK data protection authority, the Information Commissioners Office (ICO).

For any further information please email Impact Express at office@impactexpress.co.uk.