Privacy Policy

Introduction

The General Data Protection Regulation (GDPR) regulates the processing of data relating to individuals. This includes the obtaining, holding, using or disclosing of data digital records.

Southend BID shall hold the necessary data in order to perform its functions. All data held is confidential and treated with care in order to comply with the law. Lawful and correct treatment is very important to maintaining user confidence. Any data collected, recorded or used on paper, digitally or via other media platforms shall be done so fairly, will be stored safely, safeguarded and not disclosed to others unlawfully to comply with the GDPR.

The Privacy Policy contains the rules surrounding data acquisition, usage, storage and protection.

Summary of Principles

Southend BID will adhere to the Principles of Data Protection, as outlined in the GDPR.

Data will be:

- Obtained and processed fairly and lawfully and processed under certain conditions
- Be obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose
- Be adequate, relevant and not excessive
- Be accurate and up to date
- Not be kept for longer than is necessary
- Be processed in accordance with the data subject's rights
- Be kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country outside the European Economic Area (EEA)

Legitimate Interests

Stored data will be used to:

- Communicate to you, your return on investment
- Update you on Southend BID projects and initiatives
- Keep you informed with activity and in touch with the marketing team
- Contact you with information on events and involvement

Compliance relating to individuals

It is the responsibility of Southend BID to:

- Assess the understanding of obligations under the GDPR
- Identify and monitor problem areas and risks and recommend solutions
- Promote clear and effective procedures and offer guidance to staff on Data Protection issues
- Review business changes and determine whether registration under the GDPR is required

Data Acquisition

Any staff members acquiring data in any way are responsible for:

- Vetting – ensure compliancy
- Any data acquired for marketing purposes (email lists, phone numbers, addresses etc.) must be acquired through legal methods or from reputable suppliers. Individuals must have opted to receive marketing message

- Any purchased or rented data must be checked to ensure no individual on the list has opted out
- Before data purchase or rental, Proof of Provenance must be acquired. This document clearly states data's origin, how it has been used, moved and/or altered
- If the supplier cannot or will not supply an adequate Proof of Provenance, the services CANNOT be used
- Data will, more often than not, be acquired from the source, not a supplier. This means information is less likely to be corrupted, out of date or exposed
- However, use of supplier will not be an excuse to make a complaint about Southend BID and is protected from penalties. They MUST be International Organization for Standardization (ISO) or Direct Marketing Association (DMA) certified

Any data acquired by Southend BID or a third-party supplier that individuals have not opted into cannot be used and could potentially put Southend BID at risk of penalties from the ICO.

Data Classification

Staff members who regularly deal with personal data and store and transfer it are responsible for assessing its importance, sensitivity and classification. Recipients must be aware of the precautions.

- **Low:** Non-directly personally-identifiable, anonymous, pseudonymised non-personal (contact details) or vital information. Care of its storage, use and transference remain paramount
- **High:** Confidential, personal, CRM outputs, address targets, transaction details. Should be stored for the appropriate amount of time, password protected, encrypted and securely transferred

Data Transference

When transferring data within Southend BID or externally between yourself and other individuals, ensure that:

- Recipient(s) are authorised to receive. Confidential information must not be shared with unauthorised persons in any way. Doing so may lead to disciplinary action
- All reasonable steps have been taken to ensure safe transfer and use an SSH File Transfer Protocol (SFTP) and sending data by email should be avoided where possible
- Sender(s) must log the date, time, recipient, filename, format, method of transfer and classification of the data and should enable a read-receipt. They must ask recipients external to Southend BID for acknowledgement of receipt and its time
- Recipients should also log the date, time, sender, filename and type of data
- Data transfers should include details of size, layouts and amount to the recipient to provide the appropriate time to work with the files and ensure a speedier process. This should also be requested from senders external to Southend BID
- The data is to be checked against the sender's documentation as soon as possible to ensure that the sent files are correct
- Data should not be transferred outside the European Union. If it MUST be, A Company Director needs to sign off

If this is the case, ensure the following takes place:

- Information is depersonalised if it can be
- File(s) are encrypted and strong password protected
- Passwords are sent separately

- Emails should be removed from the appropriate mailboxes and folders, including the trash immediately

Data Storage

It is the employee's responsibility to ensure that all data is stored correctly. Southend BID will provide secure storage for data - archiving for electronic data (plus regular backups and cleansing) and lockable cabinets for hard copies. All devices shall be encrypted and protected with strong passwords.

Employees must ensure that personal information which they have access to is:

- Stored securely and only local for the required and appropriate time
- Encrypted and strong password protected
- Removed from any device, cloud storage platforms or company-controlled areas
- Removed from secure data – regular checks must take place
- All hard copies (e.g. personnel information and financial statements) must be kept in a secure storage and stored away when not in use. Management and the marketing team are only to have access to this
- Any breach of this may lead to disciplinary action

Breach Procedure

In the event of a data breach (loss, theft of the data itself or storage device or security breach), employees must inform management immediately to then inform Directors. The nominated members will assess the severity in order to respond correctly.

If Southend BID users have had their data compromised by an employee or third party, they shall be informed by management immediately by telephone if possible and if not, by email. If it is found that the breach was due to), disciplinary or criminal action may be taken.

Personnel records

One of the data protection rules states that it gives individuals the right to see certain information held - a fee will be at Southend BID's discretion. However, there could be a very rare occurrence where information may not be disclosed. For example, if there a document also contains personal information about another individual.

If an employee wishes to view their records, they must ask management.

Keeping your information up to date

Please help us to keep your information up to date and let us know if there are any changes to name, address, home telephone number, next of kin or emergency contact and their details and anything (medical or otherwise) required in an emergency.

Viewing your personnel record

Personal and salary records are confidential and so access to those is restricted. Under the GDPR and employment law, Southend BID is entitled to access certain records. Any request to view personal records should be made management.

There is a minimum notice period of ten working days to request to view either of these details. Files must be available as soon as possible following the notice period and, in any event, within 21 days, can only be viewed at Southend BID, Pier Offices, Western Esplanade, Southend-on-Sea SS1 1EE and must not be taken from this address.

Information that may NOT be viewed by employees

Employees may not view confidential employment references or personal data processed for the purposes of management forecasting and planning.

In addition, personal data contained within personnel files, including that where a third party can be identified, must not be viewed.

The only exceptions are:

- If the third party has consented to disclosure of information to the individual making the request
- Health records – if the third party is a health professional and has complied or contributed to said record
- If it is reasonable in all circumstances to comply with the request without the consent of the third party

Staff files are maintained by Southend BID management and are kept at Southend BID, Pier Offices, Western Esplanade, Southend-on-Sea SS1 1EE in secure storage.

Personal data will be used in connection with any aspect of the individual's employment and for no other purpose. To disclose of this to a third party without prior authorisation, may be seen as a disciplinary offence.

To update details or for a number of the policies, contact the Southend BID team via hello@southendbid.com.

Date: Thursday 24th May 2018