Data Protection Policy

Under the Data Protection Act 1998 (DPA), everyone has rights with regard to how their personal information is handled. In order to provide our services, Premiair Parking Edinburgh (PPE or we) may need to collect, store and process personal information about our current and future customers and other stakeholders (you).
PPE respects your privacy and takes its obligations concerning the privacy of data very seriously. The following policy sets out our rules on data protection and the legal conditions that must be satisfied in relation to obtaining, handling, processing, storage, transportation and destruction of personal information. To assist understanding of this policy, a list of the key terms and an explanation of their meaning under the DPA are set out in the accompanying Appendix, which is at the end of this document.

Our commitment to you
Our reputation and our on-going relationships with our customers are our most valuable assets. Our adherence to this policy will contribute to maintaining PPE's good name and its good relationships with its customers and other stakeholders.
Under the DPA, anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- processed fairly and lawfully
- processed for limited purposes and in an appropriate way
- adequate, relevant and not excessive for the purpose
- accurate
- not kept longer than necessary for the purpose
- processed in line with data subjects' rights
- kept secure
- non-transferrable to people or organisations situated in countries without adequate protection.

The DPA is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting your rights. In order to ensure that you are not adversely affected, under the DPA you have the right to:

- request access to any data held by PPE about you where PPE acts as a data controller
- prevent the processing of your data for direct-marketing purposes
- ask PPE to amend inaccurate data
- prevent processing that is likely to cause damage or distress to you or anyone else.

Any request by you to see your data may be subject to a fee to meet our costs in providing you with details of the information we hold about you.

Data security
We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Maintaining data security means guaranteeing:

- Confidentiality - only people who are authorised to use the data can access it
- Integrity - personal data should be accurate and suitable for the purpose for which it is processed
- Availability - authorised users should be able to access the data if they need it for authorised purposes.

In order to comply with the DPA, PPE has implemented the following procedures which are designed to maintain the security of personal data.
1. PPE and other group operating companies are each registered with the Information Commissioner as a data controller for the personal data that they process and keep such registrations up-to-date.
2. PPE has appointed an Information and Security Controller whose role is to ensure compliance by PPE and other

group operating companies with the DPA, this policy and any relevant operating company procedures and practices. Specific responsibilities include assessing the current knowledge of data protection within PPE and other group operating companies, ensuring that appropriate training on data protection is provided to Data Users as required and managing any data security breaches.
Any questions or concerns about the operation of this policy should be referred in the first instance to PPE's Information and Security Controller at the following address: Premiair Parking Edinburgh, 49 Eastfield Road, Edinburgh, EH28 8LS or by e-mail at premiairparkingedinburgh.co.uk.
1. Each of PPE and other group operating companies will always satisfy itself that any third party it appoints to process personal data on its behalf (such as a payroll processor or a flexible benefits administrator) understands its responsibilities under the DPA. To ensure this, PPE or the other group operating company enters into written contracts and establishes procedures with such third parties to ensure that the third party acts only on PPE's instructions and processes your personal data in accordance with the eight data protection principles set out above and PPE's practices and procedures.
There may be circumstances where PPE or another group operating company acts as a data processor on behalf of a third party, where that party is the data controller. In these circumstances PPE or the other group operating company will process such data in accordance with the instructions of that data controller.

- Each of PPE and other group operating companies will always obtain your consent before processing sensitive personal data about you.

If you are unhappy
If you consider that PPE or another group operating company has not followed this policy in relation to personal data about you, you should raise the matter with PPE's Information and Security Controller. We want to make sure that this policy is achieving its stated objectives, and we will review its effectiveness on a regular basis.

APPENDIX – key data protection terms
Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.
Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.
Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.
Personal data is defined very widely and is any data from which a living individual can be identified either from the information alone, or with other information which is in (or likely to come into) the possession of PPE. Examples of personal data include names, addresses, photographs, CCTV images of individuals, salary/job titles or opinions which allow individuals to be identified.
Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the DPA. An outline of the measures implemented by PPE in order to protect your data can be found in the policy above.
Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.
Data processors include any person who processes personal data on behalf of a data controller. PPE employees are excluded from this definition, but it could include suppliers which handle personal data on PPE's behalf (see paragraph 3 of the policy above for more information as to how we govern our relationships with third parties).
Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data (including organising, amending, retrieving, using, disclosing, erasing or destroying it). Processing also includes transferring personal data to third parties.