Data Protection Policy
Terms and Conditions

Under data protection law, everyone has rights with regard to how their personal information is handled. In order to provide our services, National Car Parks Limited (**NCP**) may need to collect, store, share and process personal information about our current and future customers, our current and future colleagues and other stakeholders.

This policy sets out NCP's approach to processing personal data.

1. Scope and Objectives

This policy applies to all NCP colleagues, volunteers, customers, contractors, trustees and suppliers. Any breach of data protection law or this policy will be dealt with under NCP's disciplinary procedure and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

All of our data processors and any third parties working with or for NCP, who have or may have access to personal information of NCP colleagues and customers, will be required to read, understand and comply with this policy. No third party may access personal data held by NCP without having first entered into an agreement or a contract with us. The agreement or contract must include data protection obligations. There must be a clause within the agreement or contract that gives NCP the right to audit compliance.

2. Our Commitment

NCP is committed to complying with data protection regulation and good practice including:

(a) only processing personal information where necessary for legitimate purposes

(b) collecting only the minimum personal information required for these purposes and not processing excessive personal information

(c) clearly informing data subjects (individuals) about how their personal information will be used and by whom

(d) only processing relevant and adequate personal information

(e) processing personal information fairly and lawfully

(f) maintaining a record of personal information processed by NCP

(g) keeping personal information accurate and up to date

(h) keeping personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate NCP purposes

(i) respecting individuals' rights in relation to their personal information, including their right of access to a copy of the information we hold on them

(j) keeping all personal information secure

(k) only transferring personal information outside the EU after gaining absolute assurance that the information can be adequately protected

(l) appropriately applying various exemptions allowable by data protection regulation

3. Responsibilities under the General Data Protection Regulation (GDPR)

3.1 NCP is a data controller, but in some circumstances acts as data processor when processing personal data. In both instances, NCP will abide by all the principles of the General Data Protection Regulation (GDPR). Please see the appendix for key GDPR terms.

3.2 Senior Management and all those in managerial or supervisory roles throughout NCP are responsible for developing and encouraging good information handling practices within NCP.

3.3 The Senior Head of Shared Services, who is also NCP's Senior Information Risk Owner (SIRO), is accountable to the National Leadership Team (NLT) of NCP for the management of personal information at NCP and for ensuring that compliance with GDPR and good practice can be demonstrated. The SIRO is accountable for security and risk management in relation to compliance with this policy.

3.4 The Data Protection Officer who the NLT considers to be suitably qualified and experienced, has responsibility for NCP's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that NCP complies with the GDPR, as do all other NCP managers in respect of data processing that takes place within their area of responsibility.

3.5 The Data Protection Officer has responsibility for producing and delivering data protection training.

3.6 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Policy and Procedure, and is the first point of call for colleagues seeking clarification on any aspect of data protection compliance.

3.7 Compliance with data protection law is the responsibility of all colleagues at NCP who process personal information.

3.8 Colleagues and customers of NCP are responsible for ensuring that any personal data supplied by them, and that is about them, to NCP is accurate and up-to-date.

4. Monitoring

This policy will be monitored by the Data Protection Officer to ensure that data protection law is adhered to.

5. Training

Colleagues, volunteers and contractors will be made aware of their obligations for data protection through effective communication programmes and yearly mandatory training. Further role specific data protection training will be provided to colleagues that handle large amounts of personal data, and/or process sensitive personal data, and/or have specialist data protection responsibilities.
All colleagues are required to complete data protection training as part of their induction training programme.

Training requirements will be reviewed on a regular basis to take account of new regulation, the needs of the individual, and to ensure that colleagues are adequately trained.

6. Register of data processed

6.1 Under the Data Protection Act 1998, NCP has notified the Data Protection Authority, Information Commissioner's Office (ICO) that it is a data controller and that it processes certain information about individuals. Under GDPR, NCP will keep a record of all data processing activities in a data inventory.

6.2 The Data Protection Officer is responsible, each year, for reviewing the details of NCP's data processing activities and updating all documented information accordingly.

7. Risk Assessment

The objective of carrying out risk assessments is to ensure that NCP is aware of any risks associated with the processing of particular types of personal information. NCP has a process for assessing the level of risk to individuals associated with the processing of their personal data. Assessments will also be carried out in relation to processing undertaken by third parties on behalf of NCP. NCP shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy and data protection law.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a risk to the "rights and freedoms" of living individuals, NCP shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Where, as a result of a data protection impact assessment (DPIA), it is clear that NCP is about to commence processing of personal information that could cause damage and/or distress to individuals, the decision as to whether or not NCP may proceed must be escalated for review to the SIRO. The SIRO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level to ensure compliance with the GDPR. DPIAs must be completed in line with the DPIA Policy and Procedure, which is on the intranet.

8. Data protection principles

All processing of personal data must be done in accordance with the following data protection principles, and NCP's policies and procedures are designed to ensure compliance with them

8.1 Personal data must be processed lawfully, fairly and transparently
The GDPR introduces the requirement for transparency whereby the data controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the individual in an intelligible format using clear and plain language. NCP fully commits to clearly communicate:

- our identity and our contact details, and the contact details of the Data Protection Officer, where applicable

- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the rights of individuals to request access, rectification, erasure or to object to processing of their data
- the categories of personal data concerned
- the recipients of the personal data, where applicable.
- where applicable, that we intend to transfer personal data to a recipient in a country that is outside of the European Union (EU) and the level of protection afforded to the data
- any further information necessary to guarantee fair processing

8.2 Personal data can only be collected for specified, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the ICO and/or in the Data Inventory Register.

8.3 Personal data must be adequate, relevant and limited to what is necessary for processing

- NCP will not collect personal data which is not necessary for the purpose or concept it is implementing
- All new data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer
- The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive
- If data is given or obtained that is excessive or not specifically required by NCP, the Data Protection Officer and departmental line managers are responsible for ensuring that it is securely deleted or destroyed in line with the Data Retention and Disposal Policy

8.4 Personal data must be accurate and kept up to date

- NCP will ensure that data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate
- NCP's departmental line managers are responsible for ensuring that all colleagues within their departments are trained in the importance of ensuring any personal data that is collected is accurate and up to date
- It is also the responsibility of individuals to ensure that their data held by NCP is accurate and up-to-date. NCP will provide customers the tools to do this
- Colleagues and NCP's customers should notify NCP of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of NCP to ensure that any notification regarding change of circumstances is noted and acted upon
- The Data Protection Officer is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors
- On at least an annual basis, the Data Protection Officer will review all the personal data maintained by NCP, by reference to the Data Inventory Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with the Data Retention and Disposal Policy
- NCP is responsible for making appropriate arrangements that, where third party may have been passed inaccurate or out-of-date personal information, to inform them that the information is inaccurate and/or out-of-date and is not to be used to make informed decisions about the individuals concerned. NCP will pass on to third parties any correction to the personal information where this is required

8.5 Personal data must be kept in a form such that the individual can be identified only as long as is necessary for processing

- Where personal data is retained beyond the processing date, it will be stored in a secure environment in order to protect the identity of the individual(s)
- Personal data will be retained in line with the retention policy as stated in the Data Retention and Disposal Policy and, once its retention date is passed, it must be securely destroyed as set out in the policy
- The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in the Data Retention and Disposal Policy, and must ensure that the justification is clearly identified and in line with the requirements of data protection regulation. This approval must be in written form

8.6 Personal data must be processed in a manner that ensures its security

8.7 Appropriate technical measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8.8 Personal data can only be transferred to a country that the European Commission deems to have an adequate level of protection for personal data (approved countries). Otherwise, personal data can only be transferred to a country outside the EU where the Information Commissioner confirms that adequate safeguards are in place or approved model contract clauses are used or exemptions apply

Safeguards

8.8.1 Adequate safeguards may be provided:

- if all parties involved in the transfer have been certified by a supervisory authority (i.e. the ICO) as having an appropriate level of protection to protect the personal data
- by complying with an approved code of conduct approved by a supervisory authority

8.8.2 Model contract clauses
NCP may adopt approved model contract clauses for the transfer of data outside of the EU. There is an automatic recognition of adequacy if NCP adopts the model contract clauses approved by the ICO.

Exceptions

8.8.3 In the absence of an adequacy decision, adequate safeguards or adoption of model contract clauses, a transfer of personal data to a country outside the EU, shall take place only on one of the following conditions:

- the individual has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the individual due to the absence of an adequacy decision and appropriate safeguards
- the transfer is necessary for the performance of a contract between the individual and the controller or the implementation of pre-contractual measures taken at the individual's request
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the controller and another natural or legal person
- the transfer is necessary for important reasons of public interest
- the transfer is necessary for the establishment, exercise or defence of legal claims
- the transfer is necessary in order to protect the vital interests of the individual or of other persons, where the individual is physically or legally incapable of giving consent
- the transfer is made from a register which according to the European Union or member state law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in European Union or member state law for consultation are fulfilled in the particular case.

9. Individual's rights

Individuals have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erase, or destroy inaccurate data
- To request the ICO to assess whether any provision of the GDPR has been contravened by a data controller and/or data processor
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller
- The right to object to any automated profiling

Individuals may make subject access requests as described in Subject Access Request Policy and Procedure. This procedure also describes how NCP will ensure that its response to the subject access requests complies with the requirements of the GDPR. All subject access requests that we receive must be forwarded to the Data Protection Officer without delay.

10. Consent

NCP understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the individual's wishes by which

he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of individuals can be withdrawn at any time.

NCP is committed to ensuring that individuals are fully informed of the intended processing of their personal data and to gain individuals' explicit consent before the processing begins. For sensitive or special category of data, explicit written consent of individuals must be obtained unless an alternative legitimate basis for processing exists.

When consent is obtained verbally for an activity/ service, NCP will log and keep a record of when the verbal consent was gained.

11. Security of data

Colleagues are responsible for ensuring that any personal data which NCP holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by NCP to receive that information and has entered into a written agreement.

Personal data must only be accessible to those who need to use it. Personal data must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, adequately protected by, but not limited to, password protection; and/or encryption of personal data stored on (removable) computer media

Colleagues are required to read and confirm understanding of the Acceptable Use Policy before they are given access to NCP information of any sort.

Manual records may not be left where they can be accessed by unauthorised colleagues and must not be removed from business premises without explicit authorisation.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Colleagues must be specifically authorised to process data off-site (where applicable).

Further rules around information security can be found in NCP's Information Security Policy.

12. Disclosure of data

NCP colleagues must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. Colleagues are trained to exercise caution when asked to disclose personal data held on another individual to a third party and they can escalate to the Data Protection Officer. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, conducting NCP business or if the information is required by law.

Data protection law permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security
- prevention or detection of crime including the apprehension or prosecution of offenders
- assessment or collection of tax duty
- discharge of regulatory functions (includes health, safety and welfare of persons at work)
- to prevent serious harm to a third party
- required by law or made in connection with legal proceedings
- to protect the vital interests of the individual, this refers to life and death situations

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

13. Retention and Disposal of Data

Personal data may not be retained for longer than it is required. Once a colleague has left NCP, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Personal data must be disposed of in a way that protects the "rights and freedoms" of individuals (e.g. shredding, disposal as confidential waste, secure electronic deletion). Hard drives of redundant PCs are to be removed and immediately destroyed before disposal. NCP's Data Retention and Disposal Policy and Procedures will apply in all cases.

14. Breach Reporting

Confirmed or suspected data breaches must be reported promptly to the Data Protection Officer. The report should include full and accurate details of the incident. Where possible the Data Breach Report form should be completed as part of the reporting process.

Once a data breach has been reported, an initial assessment will be made by the Data Protection Officer and SIRO to establish the severity of the breach. All data breaches will be centrally logged by the Data Protection Officer to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes. The SIRO will review all breaches. Breaches with a high level of severity will be reported to the ICO within 72 hours and also to the individuals involved, if deemed appropriate by the SIRO or the ICO.

NCP's Personal Data Breach Reporting Policy and Procedure will apply in all cases.

15. Complaints

Individuals who wish to complain to NCP about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer by means of letter or email. All data protection complaints we receive must be forwarded immediately to the Data Protection Officer - DataProtection@ncp.co.uk.

Individuals may also complain directly to the ICO.

Where individuals wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to NCP's Senior Risk Manager and/or further escalated to the SIRO.

APPENDIX key GDPR terms

Supervisory authority – means an independent Data Protection Authority that is empowered to uphold data protection law within the relevant territory (i.e. Information Commissioner in the UK)

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with data protection authorities.

Personal data – any information relating to an identified or identifiable living person ('data subject'); an identifiable living person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Special categories of personal data (also referred to as sensitive personal data) – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a living person, data concerning health or data concerning a living person's sex life or sexual orientation.

Data controller – the living or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or member state law, the controller or the specific criteria for its nomination may be provided for by European Union or member state law.

Data subject – any living individual who is the subject of personal data held by NCP.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a living person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the ICO and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a living or legal person, public authority, agency or body other than the data subject, controller and processor.