Privacy Policy

University of Greenwich Car Park Permit System

1. Introduction

This document explains how we 'University of Greenwich' use the personal information collected from you for the operation of the car park permit system. The policy includes how long we keep the information for and the circumstances we might share it with third parties.

2. Who holds your information?

The information is held electronically by CP Plus T/A Group Nexus as a Data Processor for the purpose of the General Data Protection Regulation (GDPR) under contract to University of Greenwich. The permit system is hosted on the Group Nexus Cloud based servers on the Google Cloud platform stored in multiple zones within the UK. It is accessed by University of Greenwich authorised staff via secure system administrator logins. The Data Controller for the purpose of the GDPR is University of Greenwich. Vehicle Registration Mark data is uploaded to the Group Nexus car park enforcement platform for the purpose of establishing authorised car park users.

3. Personal details we hold about you

We hold the data you provide when you register your details on the permit system and apply for a permit. This includes:

- name,
- university identification number,
- e-mail address,
- mobile number,
- home postcode,
- university department,
- vehicle details.
- vehicle ownership records e.g., DVLA V5 document (copy of)
- Blue Badge (copy of)

Passwords are stored in encrypted form. All data is transmitted using https secure internet connections. We need this data to establish your entitlement to a permit, contact you about your permit, and to identify your vehicle whilst in the car park.

The permit system also records when you or we transact changes to your details or permit. In addition to this, where applicable, comments may be recorded by a system administrator to provide background to changes to your permit.

4. How we use your information

We use the information held to authorise vehicle use in our car parks and manage your permit e.g., we may contact you to tell you that your permit is due to expire, or if a problem has been identified with your vehicle in one of our car parks. We may also use your details in relation to any reports of misuse or misconduct in our car parks.

If we have reason to believe that the information held is incorrect, we may change it on your behalf and notify you of this. Note incorrect information may result in enforcement action being taken against you which could result in your vehicle being issued with a Parking Charge Notice.

5. How long we hold your information

To comply with the GDPR we only hold your data for a reasonable minimum period.

We take a copy of all permit data every 12 months. Where this data relates to a financial transaction to pay for a permit, a record is held separately by the university for 7 years to comply with the Companies Act 2006. Vehicle ownership data is checked and deleted after immediately after use.

If your user account is no longer in use, then your data will be deleted from the permit system as follows:

- User account data deleted after a 1-year period has elapsed with no active permit held at any point during that period.

An e-mail will be sent to you as permit account holder warning you that your data will be deleted in 30 days if you do not respond by logging in to the system.

6. How to access your personal data

You can access and correct most of the data we hold for you by logging in to the system and amending the relevant field. If you are unable to amend data that is incorrect, please e-mail travel@gre.ac.uk with the details.

If you would like to access all the information we hold about you, you will need to make a subject access request under the GDPR. To initiate this please e-mail compliance@gre.ac.uk.

Requests for removal of data in advance of the normal protocol outlined in Section 5 above or objection to your data being processed must similarly be directed to compliance@gre.ac.uk for consideration.

7. Keeping your data secure

Your details are kept securely on the Group Nexus cloud-based servers within the UK. These servers are regularly penetration tested and access is monitored by the Cloud Monitoring and Error Reporting system with suspicious activity alerted to Group Nexus.

Daily back-up files are encrypted at source and uploaded by Group Nexus using https secure internet connection.

Report data is downloaded by the University of Greenwich periodically using https secure internet connection.

Online financial transactions are redirected to the Stripe payment system. No bank card details, or tokens are stored.

8. Sharing your personal information

To support the prevention and detection of crime we may provide data held about you to the Police, local authorities, or other statutory law enforcement agencies if requested.

25-July 2023

Ends