Security Documentation

## The data gathered by the system is as follows:

* Car number plates in parking lot and around campus
* Car build and owner
* Persons ID and Name
* Buildings/Rooms person sign in data (Date and time when they signed in)

This data will be kept for 4 years or while the person is employed/enrolled at Robert Gordan University. The data can be requested at any time, this will include any data collected by the system at that time.

Any person can ask for their data to be deleted off the system as to adhere to UK GDPR Article 17s “right of erasure”. Users will have their data deleted within 30 days of the request and be sent a conformation when their data is securely erased

All data is stored securely on Mongo DB and is encrypted to prevent data being easily accessed by unauthorised users, no data is stored on any of the hub nodes, and they are run on their own network to prevent easy access to the system. Any of the information that is accessible by users is public data, so it will not include personal information (i.e. names, date of birth, etc.) any confidential information will be stored securely and only accessible by the owner of the information or an administrator.

Under Article 5, we will only collect data that is necessary, this means we will not collect any data such as users gender, height, religion, etc. We will also keep any information up to date, and prevent any misuse of the data

### WHAT THE INFORMATION IS USED FOR

Car Data: The car data will be used to provide info on free spaces in the parking lot, it would also be used for fining anyone without a parking permit and gather data for busy hours

Sign ins: The sign in data will be used to create heatmaps of the busiest rooms in the university, this can show users free rooms without the need of having the user to go check the room themselves. The data will also be used for fire safety, fire marshals will be able to view names of personnel who were signed in, to ensure everyone’s safe

### FUTURE STEPS FOR BETTER SECURITY

We would like to work with the university and have a form to sign that would opt the student into data collection, if the student does not opt in, the data would not be stored and instead only be used for safety (i.e. fire safety)

We will also push regular updates/patches to the hubs and update the hubs OS to ensure that all possible steps are taken to minimise potential vulnerabilities. We would also ensure firewalls are installed and kept up to date and disable any unnecessary protocols and software.

The hubs would be securely locked in each room, preventing physical accesses to unauthorised users and potentially hacking into the hubs.