Surrey Heath Borough Council

Privacy Impact Assessment

Car Parking using Automatic Number Plate Recognition

Based upon the Information Commissioner's Office Privacy Impact Assessment Code of Practice

October 2014

A Privacy Impact Assessment (PIA) is a process, which assists the Council in identifying and minimising the privacy risks of new projects or policies.

Conducting a PIA involves working with people within the Council and with the people affected to identify and reduce privacy risks.

The PIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly. It is good to get any changes required into contracts at the negotiation stage.

Conducting a PIA should benefit the Council by producing better policies and systems and improving the relationship between the Council and individuals.

A Privacy Impact Assessment will aim to answer some of the questions below.

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider private.

Will the project require you to contact individuals in ways that they may find intrusive?

Name of Project: SHBC ANPR Car Park Control System

Completed by: Eugene Leal, Parking Team Leader

Date started: 31 May 2014

Date completed: 26 August 2014

Date submitted to Information Governance Manager: 22 August 2014

Privacy impact assessment

The Privacy Impact Assessment should identify particularly if any sensitive personal information is being held and how it is managed. A definition of what is defined as sensitive personal information can be found at Annex Two.

Step one: Identify the need for a PIA

The purpose for conducting this PIA is that the Fusion System will hold basic personal information in order to administer the permit system as well as vehicle registration mark (VRM) data to control entry, exit and payment for Main Square and Knoll Road multi-storey car parks. This PIA is aimed at identifying what data is collected and how it is managed from the time of collection to the time of deletion.

The Fusion System supplied by NewPark Solutions is a ticketless car park control system.

Being ticketless, the system offers the following benefits:

For SHBC:

1. Less paper used, thereby reducing running costs
2. Quicker entry time, as driver does not need to stop to collect a ticket
3. Quicker entry time also means shorter queues into the car park during busy times
4. Fewer moving parts within the pay station therefore easier and cheaper maintenance and fewer engineer callouts
5. Electronic Permit System, no need to buy or maintain pass cards.

For Customers:

6. No ticket jams
7. No lost ticket charges
8. No wet or misread tickets
9. Electronic permits, meaning no more pass card failures.
10. Quicker entry and exit through the barriers at the entrance and exit of the car parks.
11. Payments by credit/debit card
12. Expansion of payment systems to include pre-loaded parking accounts and other cashless payment options.

Fusion is an Automatic Number Plate Recognition System that captures a vehicles registration mark (VRM) and uses that information as follows:

1. Entry camera captures the VRM of all vehicles as they enter the car park and stores the information on the server.
2. Paying customers, when they are ready to pay for their parking, enter their VRM in to a pay station. The Fusion system cross-refers this VRM

to the captured database and displays the parking fee payable.

3. The parking fee is payable by cash or debit/credit card. The debit/credit card information is not stored in the Fusion system. CreditCall, who administer the payments, stores the debit/credit card information separately.
4. At the exit, an exit camera captures the VRM. This VRM is checked against the permit database and entry database. When a valid permit or payment is verified, the barrier raises.

Permit holders have to provide the VRM's of all vehicles they may use. Only basic details are held on the Fusion System and no one outside SHBC Business Services, IT section and NewPark, who are required to see the information, will have access to this permit holder's information. All permit applications forms are on-line with the appropriate instructions, declarations and signature block. A sample copy of a permit application is in Annex 3. Please follow this link for information about the system: http://www.surreyheath.gov.uk/transport/carparking/default.htm
Paying customers are advised at the entrance of the car parks that an ANPR system is in operation. Should they not wish to enter the car park they are able to continue to the highway without entering the car park.

Notwithstanding the above, for non-permit holders the only information held is the VRM of the vehicle. It is not possible to identify an individual or garner any additional information about the vehicle from the Fusion system.

Neither SHBC nor NewPark Solutions have any authority to request driver details from the DVLA for any vehicle captured by the Fusion System.

Step two: Describe the information flows

Paying Customers:

1. As the vehicle approaches the entry barrier, the entry camera captures and stores on the server the VRM, the date and time of entry and then raises the barrier to allow access in to the car park.
2. At the pay station, the driver enters their VRM. The Fusion System calculates the duration of the stay and displays the payment due. The driver pays the amount due and proceeds to their vehicle.
3. As the driver approaches the exit barrier, the exit camera captures the VRM and verifies that payment has been made then raises the barrier. The driver must exit the car park within a grace period which will vary, depending upon operational necessity.

Permit Holders:

1. The permit applicant supplies personal details, including their VRM(s), to establish their entitlement to a permit.
2. The VRM is stored on the Fusion System in the Permit Database for as long as the permit is in issue, after which it is deleted after 28 days with back-up data being deleted 7 days later.
3. As the vehicle approaches the entry barrier, the entry camera captures and stores the VRM, the date and time of entry and then raises the barrier, if the vehicle is on the Permit Database.
4. As the driver approaches the exit barrier, the exit camera captures the VRM and verifies that the vehicle has a permit then raises the barrier.

Visitors and Volunteers

1. The visitor/volunteer will supply their name and their VRM to establish their entitlement for free entry out of the car parks.
2. The VRM is stored on the Fusion System in the Discount Database.
3. As the vehicle approaches the entry barrier, the entry camera captures and stores the VRM, the date and time of entry and then raises the barrier.
4. As the driver approaches the exit barrier, the exit camera captures the VRM, checks the database to verify that the vehicle is entitled to free parking and then raises the barrier.
5. The VRM and details of their stay will be recorded manually for accounting and audit purposes.

Retention and disposal of data

NewPark Solutions store all VRM data on three secure servers held in the UK. Access to this data is restricted to SHBC personnel and NewPark Solutions support personnel as part of the Software Maintenance Agreement dated 24th March 2014.

Surrey Heath Borough Council will issue instructions to NewPark to delete VRM data held in the payment and discount databases after 28 days and to delete all permit data, including personal details, 28 days after the expiry of

the permit.

NewPark Solutions will delete all data held (for paying customers, visitors and volunteers) after 28 days, with back up discs being over-written 7 days later. NewPark Securities Limited shall carry out its duties as Joint Controller, as defined by the Data Protection Act 1998, with Surrey Heath Borough Council in accordance with Section 13.3 of the Software Maintenance Agreement signed between NewPark Securities Limited and Surrey Heath Borough Council.

The VRMs on the Permit database will be stored for 28 days beyond the expiry of the permit. Visitor and volunteer data deleted from the Discount database after 28 days, with back-up tapes over-written 7 days later.

Visitor and Volunteer data will be used to ensure the integrity of the Discount Scheme; monitoring the costs of parking and enabling, the internal recharging of the relevant parking costs. This is a new function available to Surrey Heath Borough Council and is used to provide an additional service and allow closer financial monitoring.

Access to the data will be restricted to:

Business Services, part of Surrey Heath Borough Council in the routine processing of permits, payments, refunds, system maintenance and monthly visit/volunteer audits and parking reports.

IT Services, part of Surrey Heath Borough Council for system maintenance and support.

NewPark Solutions, Support Team for periodic investigation of faults, routine maintenance, upgrading of user protocols and expansion of facilities in support of SHBC Parking Services.

Monthly Audits of Visitor and Volunteer use will be undertaken by Business Services to ensure the correct use of the schemes to enable internal recharging for the relevant parking costs.

As the Fusion system records each VRM separately, it is possible to run reports to monitor individual vehicles to ensure the Fusion system is correctly used.

Management reports will only use anonymised data to provide information such as usage, length of stay, parking fee analysis etc.

The system will not hold any personal sensitive information.

A dissemination of personal data disclaimer is on all permit applications forms.

ANPR signing is at the entrance to the car parks.

Consultation requirements

The VRM's captured by the Fusion System are anonymous. No driver/owner details can be garnered from holding the VRM as neither SHBC nor NewPark Solutions have any authority to request driver details from the DVLA for any vehicle captured by the Fusion System.

The Permit database holds basic information on the permit holder in order for that permit holder to use the car park, help Business Services to manage the permit system and to provide audit data to ensure that permits are issued correctly.

The SHBC permit database populates the Fusion Permit database with the basic information required about the permit applicant and their vehicle(s).

Internal consultation has taken place between Business Services and IT Services to ensure compliance with Data Protection Act 1998.

All permit holders have been informed of the change to an ANPR system and have been informed of how the system works. However, it has been a requirement of SHBC that any person wanting a parking permit have to supply personal details such as name, VRM, place of work and contact number in order to obtain a permit. This requirement has not changed.

Personal details for permits are required to establish the eligibility for any specific permit, in compliance with Surrey Heath Borough Council permit policy. Personal contact details are required to ensure the smooth administration of the permit system and to enable the Business Services to contact permit holders to issue reminders, chase payment and advise on changes to the parking regulations.

Step three: Identify the privacy and related risks

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
1. Holding of VRM	Possible identification to an individual from the VRM		Information Management is recorded on the corporate risk register. It is recorded as possible

2.	Parking pattern observed by Parking Services	Certain people's movements are monitored		
3.	Unauthorised monitoring of vehicle movements	As above		
4.	Back-up data, when will it be destroyed?	Information kept longer than necessary	It is not deleted in line with the retention and disposal policy	
5.	Retention period for data is not monitored and data deleted when it should be	As above	Staff do not ensure NewPark have deleted the information as required	
6.	Permit holder data maintenance procedure is not maintained	As above	As above	

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Identification of individual from a VRM	Both SHBC and NewPark do not have access to DVLA data. Any requests from the police would have to comply with Section 29(3) of the Data Protection Act	Eliminated by SHBC and NewPark. The police risk is reduced, as no information would be issued without appropriate paperwork. The data is only kept for 28 days.	The impact on the individual is reduced and is proportionate for the aims of the project

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
None		

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Review the deletion time for VRMs.	30 September 2014. Completed	Eugene Leal / Geraldine Sharman

Contact point for future privacy concerns
Eugene Leal, Parking Team Leader

Annex one

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act and in particular Article 8. If you do not understand any of the concepts please ask the Information Governance Manager.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

	Yes/No/Comment
What is the purpose of the project?	See step 1
What type of personal data are you processing and why?	See Step 1
Is any of the data classified as sensitive? If yes, please give examples of the sensitive personal data you are processing. Does it have any extra security around it? (For a list of what is sensitive personal data see Appending B)	No
How will you tell individuals about the use of their personal data?	There are details on the permits and only VRM information is collected for the operation of the Car Park
Does your processing of personal data fall within statutory powers or any other legal or regulatory duties? If yes, please specify what they are?	No
Do you have any privacy notices? If yes, do they need amending?	No
Are you setting up a new way to identify someone, or re-using an existing way?	New, identifying a vehicle only.

Does it involve using information about many people in a new or different way?	No
Have you established which conditions for processing apply?	Yes
Can someone's activities and actions now be identified as theirs, whereas prior to the project/policy they would have been anonymous (or could only be tracked back by a few people, such as in a pseudonymous approach)	No, SHBC do not have access to access to DVLA for this purpose.
Is this the sort of data that people would have concerns about?	No
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	N/A
As we are subject to the Human Rights Act, you also need to consider:	
Will your actions interfere with the right to privacy under Article 8?	No
Have you identified the social need and aims of the project?	Yes
Are your actions a proportionate response to the social need?	Yes

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

	Yes/No/Comment
Does your project plan cover all of the purposes for processing personal data?	Yes
Have you identified potential new purposes as the scope of the project expands?	Yes
Is it intrusive?	No
Are you suggesting using a lot of information about each person in a new or different way?	No
Does it involve pulling together information about people	No

from different places, linking it or cross-referencing?	
Is the data handling new or introducing change in relation to data collection?	Change
Does the project involve the use of existing personal data for new purposes? If yes, how is the use of existing personal data for new purposes being communicated to: (a) the data subject (b) the Data Protection Officer (Information Governance Manager) who will need to change the Notification with the Information Commissioner?	No
What checks are being made to ensure that further processing is not incompatible with its original purpose?	PIA
Do you have a process on disclosure of personal data to third parties? If so is it documented?	Yes. To the police

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

	Yes/No/Comment
Is the quality of the information good enough for the purposes it is used?	Yes
Which personal data could you not use, without compromising the needs of the project?	None
Could the project or policy be exempt from needing to consider privacy?	No
What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?	Quarterly in Year 1, extending to annually thereafter.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

	Yes/No/Comment
If you are procuring new software, does it allow you to amend data when necessary?	Yes
How are you ensuring that personal data obtained from	The car number

individuals or other organisations is accurate?	plates and details of the permit holders is supplied by the individual
Are you including a way to authenticate someone's identity or introducing an identity management process?	Annually for all permit holders.
Is personal data to be checked for accuracy? If yes how, and how often? Please give examples.	N/A

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

	Yes/No/Comment
What retention periods are suitable for the personal data you will be processing?	28 days
Are you procuring software that will allow you to delete information in line with your retention periods?	Yes
When data is no longer necessary for the purposes for which it was collected, how is a review made to determine whether the data should be deleted?	Data will be deleted automatically as stated above. A review will be carried out should data need to be kept.
How often is the review to be conducted and by whom?	Quarterly in Year 1, extending to annually thereafter.

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

	Yes/No/Comment
Will the systems you are putting in place allow you to respond to subject access requests more easily?	N/A
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose.	N/A

Principle 7

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

	Yes/No/Comment
Do any new systems provide protection against the security risks you have identified?	Yes
What training and instructions are necessary to ensure that staff knows how to operate a new system securely?	On the job instruction provided by supplier. Regular briefings from Team Leader to back up the training. On the job instruction for new starters from car park staff.
Does the project or policy involve more than one organisation? (including IT maintenance contractors)	Yes, NewPark Security Limited and Credit Call
Is the level of security appropriate for the type of personal data processed?	Yes
Does the system comply with the Information Security Policy requirements?	Yes
Describe the security measures that are in place to prevent unauthorised or unlawful processing of: (a) data held in automated format e.g. password controlled access to PC's (b) Data held in a manual record e.g. locked filing cabinets.	Internal audit facility incorporated in to software.
Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing? If yes, please describe the planned procedures, if no, please indicate why not?	N/A

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

	Yes/No/Comment
Is the data stored within the EEA?	Yes
Does the project or policy mean that personal information will be seen or shared?	No
If you will be making transfers, how will you ensure that the data is adequately protected?	N/A

Annex Two

Sensitive personal data means personal data consisting of information as to:

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Annex Three

To be found on the next page