

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

Guidance for the Project Manager and Sponsor

The Privacy Impact Assessment (PIA) will enable you to systematically and thoroughly analyse how your project or system will affect the privacy of the individuals (i.e. customers) involved. The templates are based on the versions produced by the Local Government Association and the Information Commissioner's Office (ICO).

- The PIA is a proactive approach to privacy protection;
- It is often the most effective way to demonstrate to the Information Commissioner's Office (ICO) how personal data processing complies with the Data Protection Act 1998;
- The outcome of a PIA should be a minimisation of privacy risk;
- Conducting a PIA would be a legal requirement under the General Data Protection Regulation (GDPR).

Further guidance on completing the Pre-Assessment and Full PIA is available from the accompanying guidance. Further information on the PIA is also available on the [ICO's PIA code of practice](#).

Section One - Project Summary

Project Name	Truckfile Workshop Management	Directorate and Service	Supporting People
Project Sponsor and Position	Josephine Allman Head of Camden Accessible Travel Solutions	Project Manager and Position	<div style="background-color: #cccccc; width: 100px; height: 15px; display: inline-block;"></div> Programme Manager <div style="background-color: #cccccc; width: 100px; height: 15px; display: inline-block;"></div> Business Lead
Project Start Date	January 2018	Project Go Live Date (anticipated/planned)	September 2018
<p>Brief Description Of The Project</p> <p>The existing fleet and servicing system, Fleet Plus (CFC Solutions), needs to be replaced as it has been deemed no longer fit for purpose. It is also costly, both in terms of regular annual vendor support payments, and charges for one-off changes and staff training. The system is very paper based, especially in relation to the management of vehicle schedules and inspections, i.e. the workshop element and there is no facility to roll out access to a wider selection of managers e.g. Transport Manager, Business Manager and Head of Service, as the system is desk top based and requires additional licenses to roll out further. As a result, the existing system poses a risk to compliance, especially in areas of evidencing all aspects of vehicle maintenance. The existing system will be replaced by fully integrated web-based Fleet and Workshop Management System. There has been a procurement process and the successful supplier has been identified, Magic Internet for their software, Truckfile.</p> <p>The system is hosted at an external data centre on dedicated servers. Magic Internet have full control over data partitioning and each client has a separate database/s. This provides the level of security and data privacy that is currently required for systems holding any personal data covered by GDPR.</p>			

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment



GOVERNANCE ARRANGEMENTS

The PIA may be subject to review and audit by Camden including the ICT Project Review Board, Corporate Information Governance Group (CIGG) and the Information Commissioners Office (ICO). You may therefore find it helpful to keep the signed PIA and all supporting documents with your project file for audit purposes.

A copy of the completed Pre-Assessment (including the signed declaration where appropriate) must be sent to the Clerk to the CIGG. The CIGG will review pre-assessments on a risk basis and at any time during the life of the project, may ask you to attend a meeting to provide further information, answer questions and respond to any privacy concerns.

The PIA may also be requested by the ICT Project Review Board and ICO at any time.

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

Section Two - About the Project

1 Identify the need for a PIA

- **What does the project aim to achieve, what benefits will it bring to Camden, to individuals and other parties?**

The new TruckFile Fleet and Workshop Management System will incorporate Fleet Management, online workshop job management, and daily vehicle compliance checking, via a combination of web-based desk top icons and the use of handheld smart device technology.

A 'driver's app' will be available on mobile devices allowing the driver to perform their requisite daily vehicle checks. This information will then be sent electronically to Fleet Management for allocation and job raising if works are required.

Benefits of the system are:

- Compliance checking will be easier
- Paperless
- Aid fitters in completing work consistently as job sheets are on a handheld computer/tablet
- Customers – Speed up throughput of vehicles, and being kept up-to-date about vehicle status and readiness for collection.
- Ensures workshop function more effective and all required steps completed as unable to progress status of a vehicle job unless completed fully.
- Increased ability to produce reports and financial information for our service and resource management and provision to customers
- Earned recognition compliant with DVSA (pilots currently being carried out)
- Delivers an efficient workshop with increased throughput and productivity – aids the identification of bottle necks and individual performance
- The outlay, support and maintenance costs are significantly below existing system, whilst delivering greater capability and future proofing.
- Cloud based system – Data storage and backup r being completed by external 3rd party
- Enables improved management of parts within the stores, due to running tally on parts used enabling speedy re-order.
- Greater suite of reports and potential for bespoke reports as required with minimal costs
- Supplier keen to work collaboratively with end users to incorporate enhancements to the system to deliver continuous improvement.
- Training for new users available and provided as and when required.

- **Why was the need for a full PIA identified?**

Driver Licence details will be held on the system to ensure Driver compliance. Driver name and address, Licence Number, Vehicle entitlement and expiry date will be held on the system. System will identify licences due to expire and any points that might impact their suitability to drive on behalf of the Council.

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

2 Describe the information flows

- **Describe the collection, use and deletion of personal data. A flow diagram can be used for ease of understanding.**

Data is initially collected through data input to the system by Camden Accessible Travel Solutions (CATS) staff:

1. Vehicles; all details relating to vehicle
2. Schedule of inspections and services
3. Drivers; Licence Number, Groups and expiry date
4. System users; Name only
5. Parts; Number, location within the stores

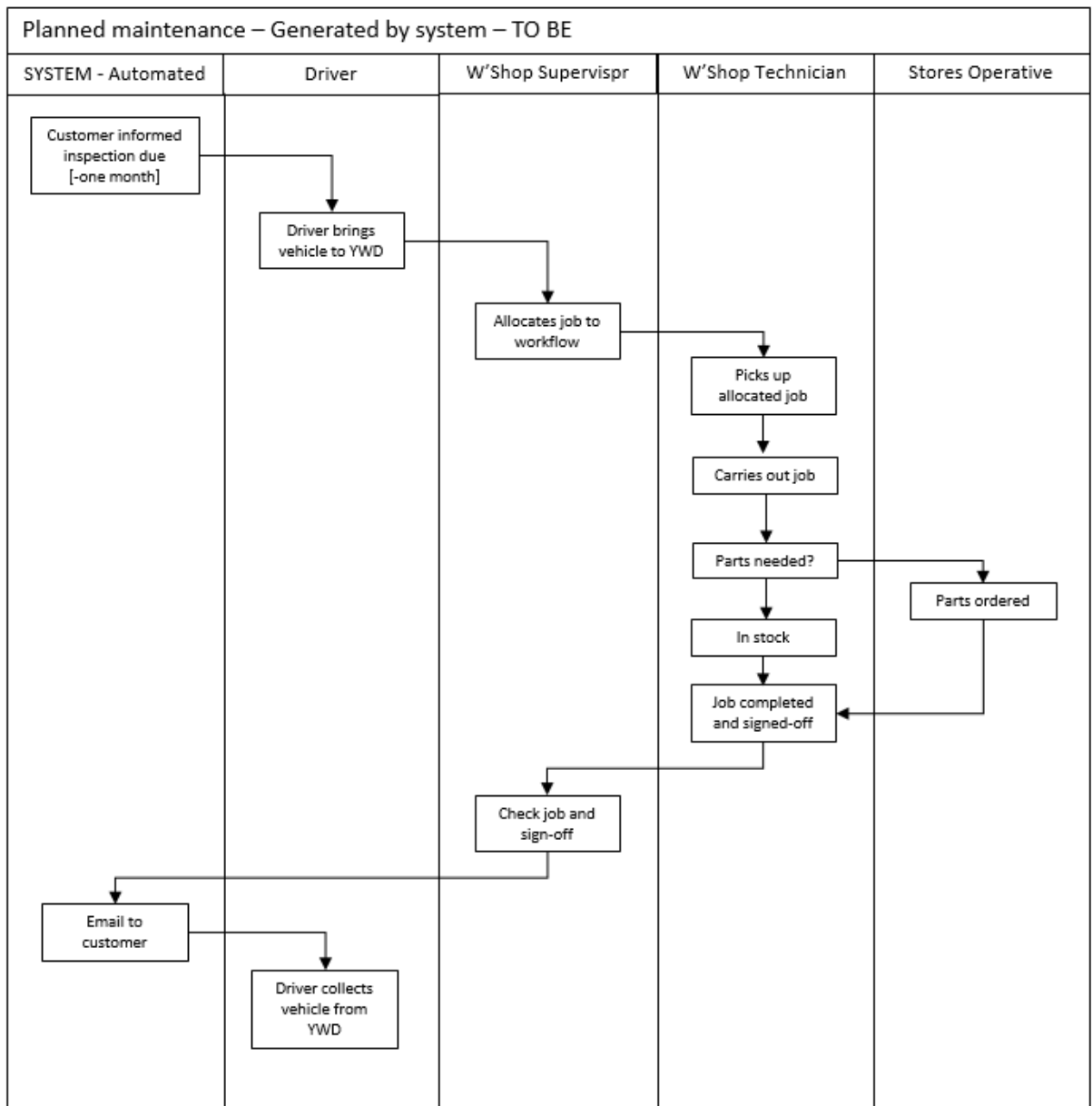
[NOTE: This information flow has not been included at this time as it is quite detailed]

Vehicle schedule information, i.e. regular inspections and MOTs, is provided to all commissioning services, e.g. CATS Passenger Services, Camden Repairs Team (CRT) to ensure vehicles are presented at the required time and not used outside of inspection or MOT compliance regime.

Although there may be some duplication of driver data with the Passenger Transport application, FlexiRoute, there is no integration or sharing of data between the two systems.

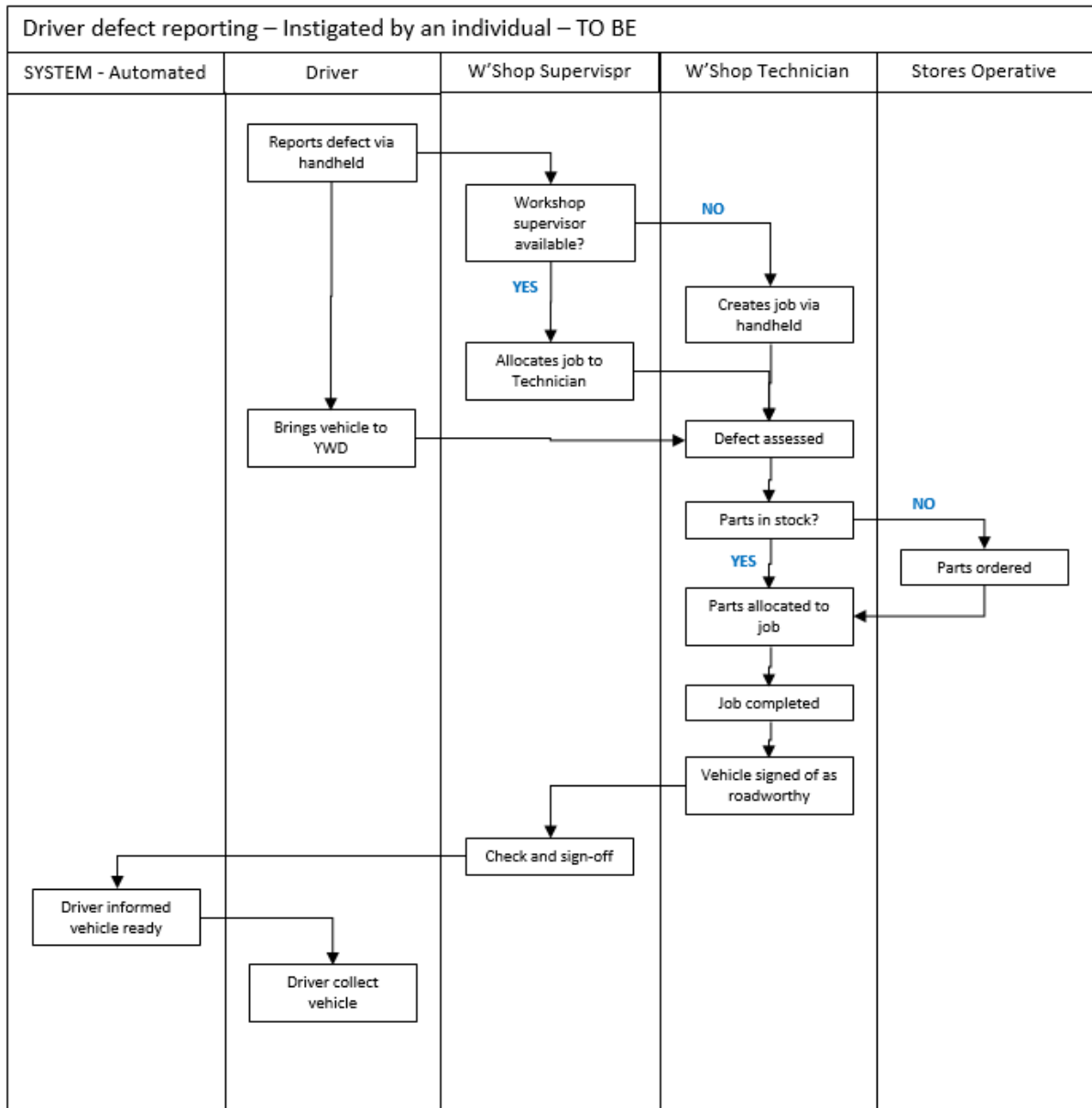
PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment



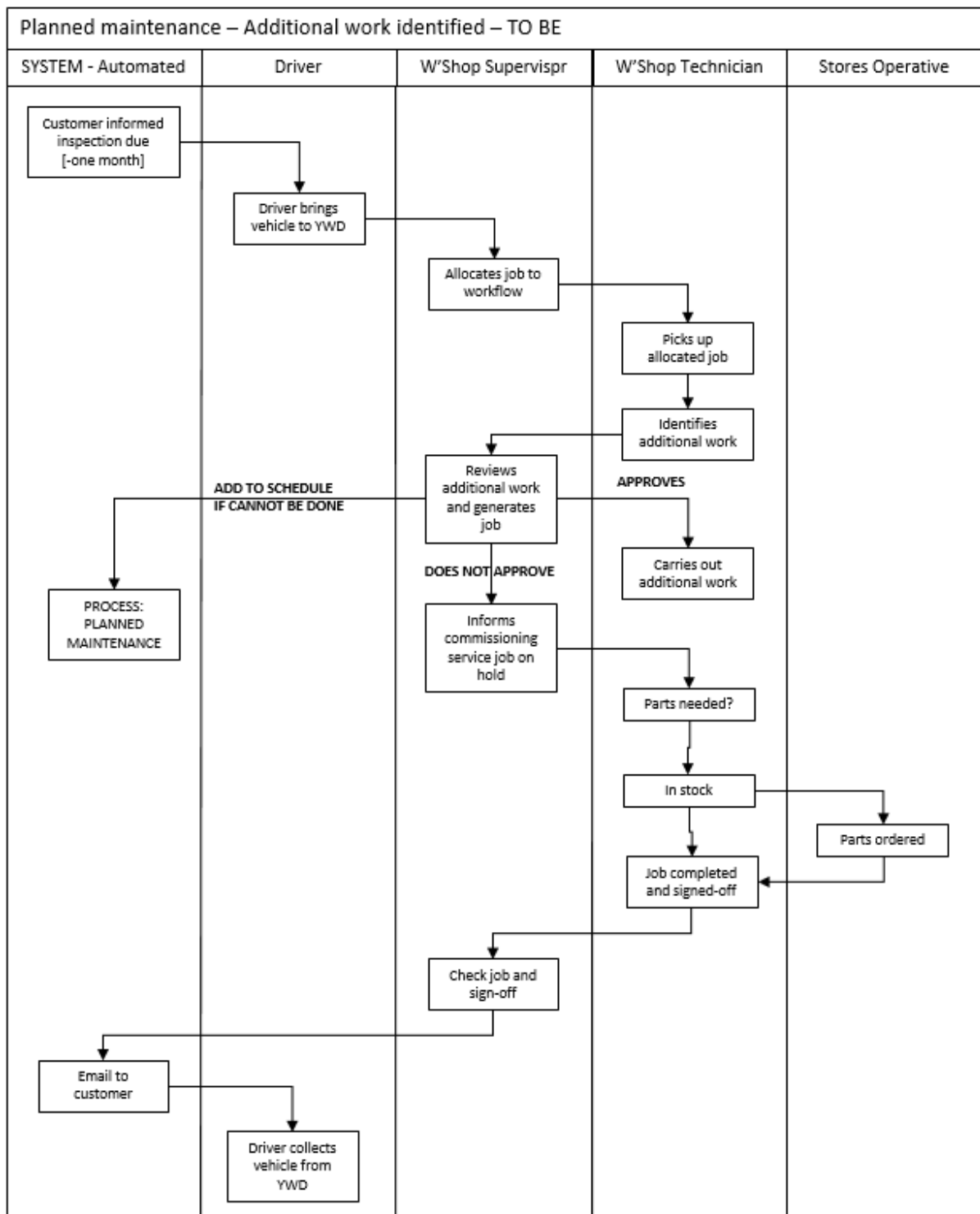
PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment



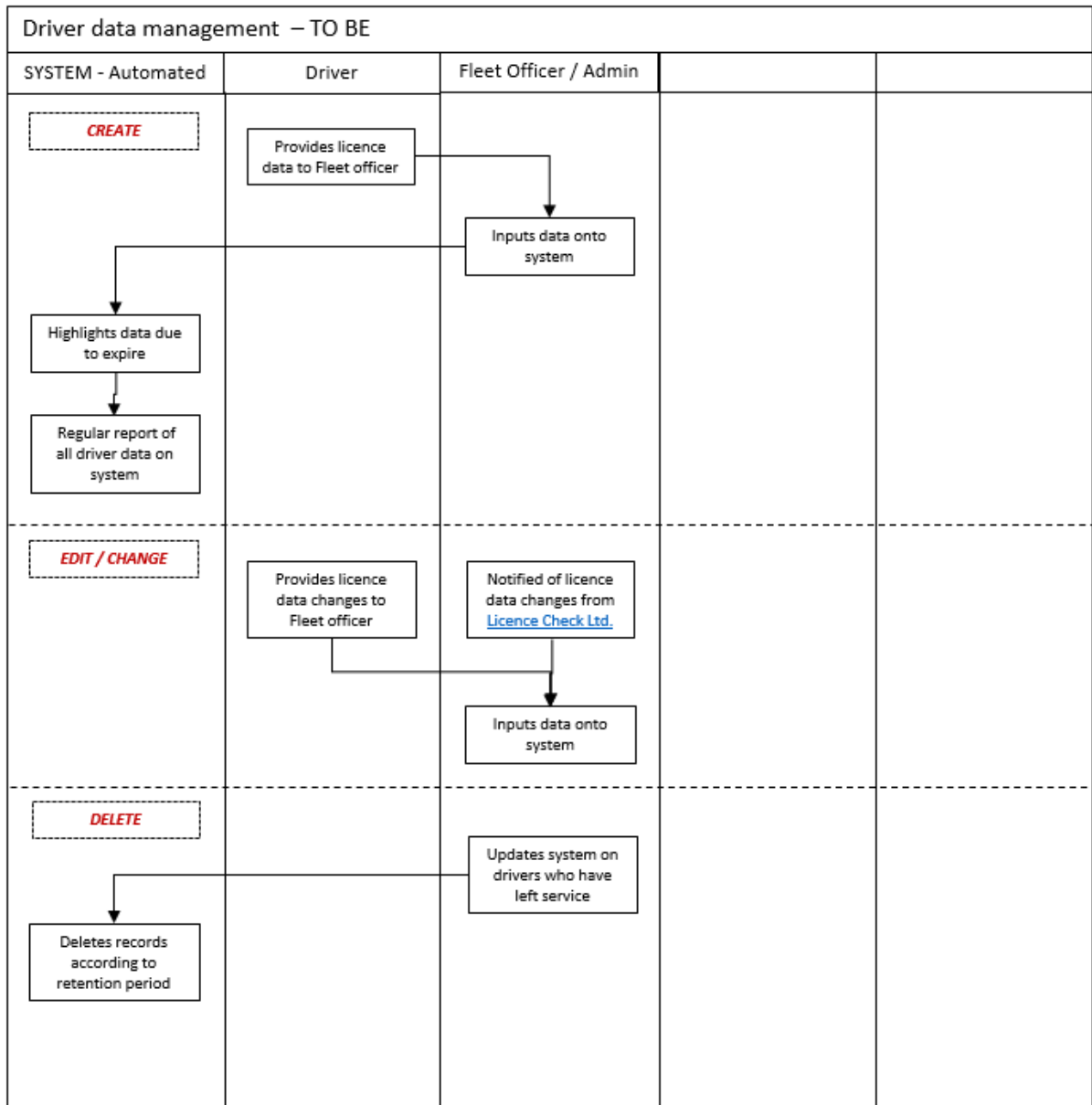
PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment



PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment



PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

How many individuals will likely be affected by the project?

c.350-400 including drivers, managers, workshop staff, IT support, business and performance staff.

3 Consultation requirements

- **What practical steps will you take to ensure that you identify and address privacy risks?**
- **Who should be consulted, internally and externally?** It may be helpful to link to the stages of the project.

Response:

We will consult with Camden Information and Records Management team to request for their expertise in this particular area and ensure we have covered all potential risks. Completing this assessment will help us identify and address any potential privacy risks.

We will need to consult with the following groups/individuals:

- **Drivers**
- **Trade Unions**
- **Fleet and Workshop operatives**
- **Relevant Managers and Supervisors**

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

Section Three - Data Protection Compliance Questionnaire

Use this questionnaire to help ensure that the project and the manner in which it will process personal and sensitive personal data in compliance will comply with the Data Protection Act. The questionnaire contains 60 questions of which 44 are closed (Yes/No).

This questionnaire is intended to be dynamic and updated/amended as you progress through the project. It is therefore recommended that you start completing this at the start of the project to ensure you have all key controls in place before the project goes live.

If you have answered NO to any of the questions you may find it beneficial to record these in the Issues and Risk Log in section six to record and monitor mitigating actions whilst you are in the process of implementing them. You can amend this table to better suit your project or incorporate it into your overall project risk register.

Further guidance on completing the Pre-Assessment and Full PIA is available from the accompanying guidance. Further information on the PIA is also available on the [ICO's PIA code of practice](#).

<u>Principal 1 - Fair And Lawful Processing</u>			
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.			
1	<u>Schedule 2 - Grounds for Legitimate Processing of Personal Data (see Section Four for conditions for processing)</u> What type of personal data are you processing? Please list the categories you can use the information from the pre-assessment).		<ul style="list-style-type: none"> • Drivers personal details <ul style="list-style-type: none"> • Name and address, licence type, licence group, license number. • System user name
2	Is there a legitimate basis for processing the data? If YES then please briefly explain the legal basis. If NO then please explain the basis on which the data is being processed?	YES	<p>The data outlined in Q1 is required in providing our driver compliance and insurance duty for the provision of transport to vulnerable adults and children and in ensuring that only staff with the requisite licenses drive Council vehicles.</p> <p>It follows the rules and guidelines in the Office of the Traffic Commission Vehicle Operator Licensing rules and regulations.</p>
3	<u>Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data (see Section Four for conditions for processing)</u>	NO	

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

	<p>Will you be collecting <i>sensitive personal data</i>, e.g. ethnicity, religion, health, sexuality, criminal conviction and trade union</p> <p>Please list all the data categories (if not already done so in question 1).</p>		
4	<p>Is there a legitimate basis for processing the sensitive personal data?</p> <p>If YES then please explain.</p> <p>NO then please explain the basis on which the data is being processed.</p>	N/A	
5	<p>If you are relying on different grounds for different categories of sensitive personal data (e.g. a different basis for each type of data collected) then please explain.</p>	N/A	
6	<p><u>Obtaining Consent</u></p> <p>Are you relying on the individual to provide consent to the processing of their personal data (as grounds for satisfying Schedule 2)?</p> <p>If YES then how and when will this consent be obtained?</p> <p>If NO then what legitimate arrangements are already in place?</p>	NO	There is no reliance on consent, the council relies on the legal obligations outlined in Q2.
7	<p>For <i>sensitive personal data</i> will you ask for explicit consent from the individual (as grounds for satisfying Schedule 3)?</p> <p>If YES then how and when will this consent be obtained (answer only if different from question 6)?</p> <p>If NO then what legitimate arrangements are already in place?</p>	N/A	Same as above
8	<p><u>Lawful Processing</u></p> <p>Does your processing of personal data fall within your statutory powers?</p> <p>If NO then why not?</p>	YES	
9	<p>How will you ensure compliance with the Human Rights Act (Article 8)?</p> <p>http://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/1/chapter/7</p>	YES	The data will be stored on an IT system that is only accessed by staff that require the data to carry out their work duties. Staff understand data confidentiality through training and agreeing to comply with the IT Code of Conduct policy as part of their terms and conditions on employment to the Council. The system will only hold information about Camden staff as the system is for Camden Council only.

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

10	Have you assessed whether any of the personal data being processed is held under a duty of confidentiality, e.g. client confidentiality? If NO please explain.	YES	
11	Have you assessed whether your processing is subject to any other legal or regulatory duties? If YES please list the additional legal or regulatory duties and how you will comply with these. If NO please explain.	YES	As a Transport operation, we must comply with the Operator Licence regulations, which ensures that all of our drivers have the appropriate licences. We are also required to ensure compliance with Drivers Working Hour Regulations to log drivers working hours.
12	<u>Fair Processing</u> Will you make individuals aware of the identity of your organisation as the data controller and that they are holding personal data? If YES then please state how and when. If NO then please explain.	YES	Prior to driving a Council vehicle there is a requirement to undertake a Driving Assessment, undertaken by approved staff within CATS. On application for a driving assessment, the individuals will be made aware that the Council will be holding their data.
13	Will you notify the individual on how their personal data is being used? If YES then please state how and when. If NO then please explain.	YES	When an individual's driving assessment is complete the driving assessor informs the individual that the information collected will be used for the purpose of driver compliance.
14	Will you receive information about individuals from third parties? If YES then please give examples.	Yes	DVSA, Occupational Health, GP or Police, in relation to fitness to drive.
<u>Principle 2 - Purpose Limitation</u> 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.			
15	<u>Uses of Personal Data within the Organisation</u> Will you have a procedure for maintaining an up to date record over the use of personal data?	YES	Staff are required to inform the Council of any material change that might affect their ability to carry out their duties (including driving) and to ensure that the information on their driving licen is up to date eg change of name or address. The service will undertake periodic license checks to ensure compliance. However, there is an obligation on staff to proactively report and provide relevant data as soon as practical.

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

16	<p><u>Use of Existing Personal Data for New Purposes</u></p> <p>Does the project involve the use of existing personal data for new purposes? If NO then go to question 18.</p>	NO	No personal data will be used, however anonymised data may be used for reporting trends and performance, eg age spread of license holders
17	<p>What checks have you made to ensure that processing of personal data is not incompatible with its original purpose?</p>	N/A	
18	<p><u>Disclosures of Data</u></p> <p>Is there a corporate disclosure policy that covers the data processed under this project? If YES then then please skip to question 20.</p>	YES	
19	<p>If NO to question 18 then will you produce an appropriate disclosure policy? If NO the please explain.</p>	N/A	
20	<p>How will your team be made aware of the disclosures policy with respect to handling disclosures?</p>		Staff receive training and information is readily available on the Councils intranet.
21	<p>How will individuals be made aware of disclosures of their personal data?</p>		The service will inform the individual formally in writing.
22	<p>Where a 3rd party is involved, have you assessed their compatibility with respect to their use of the personal data in question (e.g. compatibility of systems, conflict of interests etc.)? If NO then please explain.</p>		Magic Internet Technologies Ltd are registered with the Information Commissioner's Office (ICO) as a Data Controller under the Data Protection Act - Registration Reference A8280195. We have reviewed their relevant company policies as part of the IT procurement exercise as well as considered the technical security of the system and data held before awarding a contract.
<p><u>Principle 3: Adequate, Relevant And Not Excessive</u></p>			
23	<p><u>Adequacy and relevance of Personal Data</u></p> <p>What arrangements/procedures are in place to determine the adequacy and relevance of the personal data being collected for each purpose, and to ensure that it is not excessive (e.g. ensuring that only minimum required amount of data is collected for verification)?</p>		<p>Only data that is relevant to the provision of the service is collected e.g.</p> <p>Drivers – only data relevant to their availability and necessary license applicability is held</p>
24	<p>What arrangements are in place to ensure that data collection procedures are and will remain adequate, relevant and not excessive in relation to the purpose for which data is being processed?</p>		Annual reviews of the system data and regular reviews of service needs.

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

Principle 4: Accurate And Up To Date			
Personal data shall be accurate and, where necessary, kept up to date.			
25	Please list all the sources of personal data being processed, i.e. internal systems, individuals, third parties etc.		Individuals via transport driving assessments carried out by CATS driving assessors
26	Have you assessed the risk to the individual and data controller with respect to the consequences that could be caused through; 1) Inaccuracy of data and; 2) Holding data that is out of date? If NO then please explain.	YES	If we hold inaccurate data, the consequences could lead to drivers not being allowed to drive as the system could show an inaccurate licence expiry.

The onus of up to date data is on both the commissioner and our service. There is reliance on the customer/commissioner to provide the up to date data but the transport team will ensure it remains up to date by updating the record.

27	What arrangements are in place to check the accuracy of the data with the individual?		The service carries out periodic reviews of the staff to ensure we hold up to date information.
28	Will accuracy checks cover free text fields including comments about individuals?	YES	
29	How will you determine when and how often personal data would require updating?		Service management, in contact with drivers on a regular basis will also flag ad-hoc changes needed or the individual will contact the service to inform us directly.
30	What arrangements are in place to for individuals to notify you if they believe their data to be inaccurate?		Individuals can contact CATS and inform the service of any inaccuracies which will then be investigated and corrected on the system.

Principle 5 - No Longer Than Necessary			
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.			
31	Retention Policy Is there a corporate data retention policy that covers the data processed under this project? If YES then skip to question 33.	YES	
32	If NO to question 31 then will you produce a suitable retention policy?		

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

	If NO the please explain.		
33	How will you determine when the data is no longer necessary for the purposes for which it was collected? Who will be responsible for reviewing the data?		Drivers leave service. Leaver's procedure. Service manager
34	If the data is held on an IT system then will this system flag records that due for review/deletion? If NO then please explain (answer only if different from that stated in question 35).	NO	
35	Will there be any exceptional circumstances for retaining certain data for longer than the normal period? If YES then please explain.	NO	
36	<u>Destruction of personal data</u> Are there arrangements over the secure deletion/destruction of personal data? If NO then please explain.	YES	External supplier has policies in place relating to the secure deletion/destruction of personal data.
<u>Principle 6 - Data Subject Access</u>			
Personal data shall be processed in accordance with the rights of data subjects under this Act.			
	<u>Subject Access</u>		
37	Is there a corporate procedure that deals with subject access requests under this Principle? If YES then please skip to question 42.	YES	
38	If NO to question 37 then will you introduce a procedure? If NO the please explain.	N/A	
39	How will you locate all personal data relevant to a request (including any appropriate 'accessible' records)?		By searching on the system or requesting an individual report
40	Will you provide an explanation of any codes or other information likely to be unintelligible to a data subject (e.g. short codes or abbreviated codes)? If NO then please explain.	YES	
41	Are there arrangements in place to manage personal data relating to third parties? If NO then please explain.	N/A	
	<u>Withholding of personal data in response to a subject access request</u>		

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

42	Will there be any circumstances where you would withhold personal data from a subject access request? If YES then on what grounds would and how would this be identified?	NO	
43	<u>Processing data that may cause Damage or Distress</u> How will you avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?		The data will not be available to staff who have not been trained in the use of the data. Any data transferred is done so securely to ensure that the individuals' data is not at risk of falling into the wrong hands.
44	<u>Right to Object</u> Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing? https://ico.org.uk/for-organisations/guide-to-pecr/introduction/what-are-pecr/ If NO then please explain.	NO	There is no intention to use individual data from the Truckfile system for direct marketing.
45	<u>Automated Decision-Taking</u> Are any decisions affecting individuals made solely on processing by automatic means?	NO	
46	If YES to question 45 then will you notifying the individual that an automated decision making process has been used? If NO then please explain.	N/A	
47	<u>Rectification, Blocking, Erasure and Destruction</u> Are there (e.g. corporate) procedures or will you have a procedure for responding to a data subject's notice (in respect of accessible records) or a court order requiring rectification, blocking, erasure or destruction of personal data? If NO then please explain.	YES	There is a corporate Subject Access request procedure under the Data Protection Act. Other GDPR rights will be dealt with via requests to the DPO. For example users will be able to delete/rectify records etc. Data portability is not required.
<u>Principle 7 - Data Security</u>			
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.			
48	<u>Security Policy</u> Is there a corporate security policy that covers the protection of personal data and processing activities under your project? If YES then please skip to question 50.	YES	

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

49	If NO to question 48 then will you produce a policy? If NO the please explain.	N/A	
50	Who will be responsible for enforcing compliance with the security policy?		Data owners – the Information Asset Owner Securities team (ICT)
51	<u>Unauthorised or unlawful processing of data</u> What security measures are in place to prevent any unauthorised or unlawful processing of data held manually (e.g. locked cabinets) and on IT systems (e.g. passwords)?		User roles are defined and administrative access is limited to Corporate SSI team (ICT) so it is separately managed from the CATS service. The server that hosts our data is specifically assigned to Camden and is accessed by a unique login ID which is entered on log in.
52	Are there separate measures to protect sensitive personal data? If NO then please state why the measures in question 51 are sufficient.	NO	Sensitive personal data will be limited by assigned user access roles.
53	Is there a corporate procedure for detecting and reporting breaches of security (remote, physical or logical) relating to this project? If YES then please skip to question 55.	YES	
54	If NO to question 53 then will you introduce a procedure? If NO the please explain.	N/A	
55	<u>Contingency planning - Accidental loss, destruction, damage to personal data</u> Have you assessed the risks and put in place mitigating controls to minimise the risk of data loss through: <ul style="list-style-type: none"> • Human error or theft; • Computer virus or network failure; • Fire, flood or any other disaster? If NO then please explain.	YES	The service is covered by the council's IT policies, Magic Internet Technologies Ltd etc. This is considered proportionate in comparison to the risk levels.
56	Do you have procedures to recover data (both automated and manual) in the event that data is lost? If NO then please explain.	YES	The supplier will take daily backups at both the data centre and additional off site storage systems. Data Images Security Incident & Computer Misuse policy http://teams.lbcamden.net/teams/bi/Transport%20Project/ITMS/ITMS%20Procurement%20documents/Dat

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

			a%20Images%20(Flexiroute)/DIS016%20Security%20Incident%20and%20Computer%20Misuse%20Policy.pdf Should any equipment be lost/stolen e.g. mobile devices and laptops, the unique login credentials as well as system timeouts, should prevent loss of data. There should be no requirement for printed data.
<u>Principle 8 - Overseas Transfer</u> There is no need for the Council to transfer data out of the EEA itself. If the Council is using third party systems e.g. survey tools, then care should be taken to check no data is being transferred out of the European Economic Area.			
57	<u>Direct transfer</u> Will you be transferring personal data to a country or territory outside of the EEA? If YES then please state where and with whom.	NO	
58	If YES to question 57 then have you assessed whether the country or territory has adequate privacy protections in line with EEA? If NO then please explain.	N/A	
59	<u>External agents</u> Are you working with an external system provider (i.e. web based service) for the processing of personal data?	YES	
60	If YES to question 59 then is the provider hosting your personal data on servers outside of the EEA? If NO then please explain.	NO	Servers are hosted in the Datatech site in England.

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

Section Four - Conditions for Processing

The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. At least one of the conditions listed above must be met whenever you process personal data. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle.

Schedule Two Conditions	Schedule Three Conditions
<ul style="list-style-type: none"> The individual whom the personal data is about has consented to the processing. 	<ul style="list-style-type: none"> The individual whom the sensitive personal data is about has given explicit consent to the processing.
<ul style="list-style-type: none"> The processing is necessary: <ul style="list-style-type: none"> - in relation to a contract which the individual has entered into; or - because the individual has asked for something to be done so they can enter into a contract. 	<ul style="list-style-type: none"> The processing is necessary so that you can comply with employment law.
<ul style="list-style-type: none"> The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions. 	<ul style="list-style-type: none"> The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition
<ul style="list-style-type: none"> The processing is in accordance with the “legitimate interests” condition. 	<ul style="list-style-type: none"> The individual has deliberately made the information public.
	<ul style="list-style-type: none"> The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
	<ul style="list-style-type: none"> The processing is necessary for administering justice, or for exercising statutory or governmental functions.
	<ul style="list-style-type: none"> The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

PRIVACY IMPACT ASSESSMENT
Annexe 2 - Full Assessment

Section Five - Conclusion and Declaration

Please complete the declaration below. Retain this document and supporting evidence with your project file.

PRIVACY IMPACT ASSESSMENT – DECLARATION OF COMPLETION

I declare that I have completed the Privacy Impact Assessment to the best of my knowledge. I and in the process of or have implemented the actions arising from this PIA to ensure that the project and the processing of personal data complies with the Data Protection Act 1998.

I understand that the privacy impact assessment and any supporting evidence may be required for review and audit by Camden including the ICT Project Review Board, Corporate Information Governance Group, and the Information Commissioners Office. I also understand that these groups may and at any time during the life of the project may ask me to attend a meeting to provide further information, answer questions and respond to any privacy concerns.

Project Manager Signature and date		Alternately email approval can be attached
Project Sponsor Signature and Date		

PRIVACY IMPACT ASSESSMENT

Annexe 2 - Full Assessment

Section Six - Issues and Risks Log

Use the risk register as a template to record risks and mitigating actions arising from your PIA, and monitor their implementation. You can amend this table to better suit your project or incorporate it into your overall project risk register. You may also find it helpful to group your risks under each DPA principle.

The accompanying guidance document includes a section entitled “Data Protection Act Principles”. This may further help you to identify the key risks associated with the protection of personal data and non-compliance with the Data Protection Act.

	Issue or Risk	Proposed Action/Control	Risk/Action Owner	Timescale for implementation
	Principle 1 - Processing of data			
	Principle 2 - Obtaining data			
	Principle 3 - Adequacy of data			
	Principle 4 - Accuracy of data			
	Principle 5 - Data retention periods			
	Principle 6 - Rights of the individual			
	Principle 7 - Technological safeguards			
	Principle 8 - Transfer of data outside the EEA			