DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The General Data Protection Regulation (GDPR) introduced a new mandatory requirement for organisations to identify and then assess high risks to the rights and freedoms of individuals associated with any proposals to process personal data, particularly special category personal data. Please refer to the Council's Privacy by Design Policy.

Below is set out a template DPIA form which users are expected to **save a copy** and complete. The form is divided into three parts. Part One should be completed **first**. If necessary, Parts Two and Three should then be completed. Each Part contains further guidance and instructions. Part Three is divided into three sections. You are advised to read the instructions before completing the form.

Instructions on how to complete DPIA

NB: For any DPIA's relating to Adult Social Care/Children's Services and Public Health (ASC/ChS/PH) please contact Mazidur Rahman, Information Governance/Caldicott Support Manager, at Mazidur.Rahman@rbkc.gov.uk who can support you in this process.

1. Seek advice from the statutory Data Protection Officer [DPO] on if you need to complete a DPIA.
2. Obtain a copy of the DPIA Form from the DPO website
3. Contact the Information Management Team [IM Team] or DPO to obtain a unique reference number
4. Complete the DPIA Screening Section – Part One
5. If you answer **No** to any of the screening questions, liaise with the IM Team or for ASC/ChS/PH the IG/Caldicott Support Manager to confirm and then arrange for your head of service or project sponsor (whichever is appropriate) to sign this off.
6. Maintain a copy of Part One in your project folder and send a copy to the IM Team for entry onto the DPIA Register so that this can be recorded against your project
7. If you answer **Yes** to any of the screening questions go on to complete Part Two, and then the risk assessment in Part Three.
8. Complete the DPIA form and liaise with the IM Team to agree mitigations and record actions to be taken to reduce any identified risks. This also includes agreeing timescales for either completing mitigation actions and/or keeping the risks under review.
9. Obtain recommendations from the IM Team or the DPO (whichever is appropriate), add these to your form and send to your Head of Service or project sponsor for final sign off as Information Asset Owner (IAO).
10. Attach a copy of your completed Parts 1-3 of the DPIA to your project folder.

11. Send a final copy of your completed DPIA to the IM Team who will maintain a record of it in the council's DPIA Register
12. If you are required to implement or review your mitigations against an agreed timetable, please include these in your DPIA action plan and complete the online Review Actions columns against your registered DPIA
13. All queries about the DPIA should quote the DPIA Unique Reference Number.
14. Details of all relevant council policies and guidance can be found on the DPO and IM Intranet Pages
15. See image below to guide you through the points that need to be considered when completing the DPIA

Please Note:

- We have tried to make the questions as clear as possible. Please read the guidance next to each question.
- Where appropriate the Respond column contains further guidance, as that will provide you with further insight on what you are being asked to consider. You should write over it when providing your response
- We also ask that you complete the description, so that a full picture of what you aim to do, what you aim to process, and what outcomes you expect are captured
- If a question is Not Applicable just say N/A
- The DPIA relates to the intended processing. If new processing happens following sign off, you can always amend or update your DPIA.

Understanding Your Project Before you start to complete the form use your knowledge of the project/procurement/ initiative to describe the purpose of the project and what are the expected outcomes. How big is this project? Are you expecting to process a lot of information about people. Consider the sources of the data you plan to use. Is it internal and will your project change how it is used. What is the likely impact on individuals with respect to the service they will receive, and have you considered any pitfalls that could negatively affect an individual/s
Understanding Your Intended Processing What system/tools do you think you will need to deliver your intended purpose. Is it internal or will you have to procure it, or ask a contractor to provide it? You should also think about where the data will be stored – internally on the council's network, by a third party provider on their premises (data centre) or cloud platform? the type of information it requires,. who you will share their data with and what outcomes you hope to achieve.

PART ONE: DATA PROTECTION IMPACT ASSESSMENT [DPIA] - SCREENING QUESTIONS

DPIA Screening Questions to determine if a DPIA is needed. If the answer to any of these questions is yes, users **must** complete Part Two Data Protection Checklist and Part Three Data Protection Risk Assessment. If the answer is **No** to **all** the questions in Part One, you do not need to undertake the rest of the DPIA. In Part One Use the end column (Description) to provide additional information

DPIA Reference Number: [TBC]	
Project Title	Award Report for Statutory Documentation Printing Services and Parking Remittance Processing and Document Scanning Service (Parking Services)
Process Owner/Project Sponsor	Vania Franco
Author (person completing this DPIA)	Alex Mummery
Owning Department and Team Name	Parking Services – Contracts & Systems Team
Date Completed	Click or tap to enter a date.

Provide a brief Description of your project. What is it about, what do you hope to achieve. What stage are you at in the process. Who your key stakeholders are and who is your intended recipients or services
The purpose of this project is to allow the continuance of two key services for parking services as both current service provider contracts have expired. We are currently at the stage of seeking a waiver and an approval for two direct awards to the existing service providers covering the contract for Statutory Documentation Printing Services and Parking Remittance Processing and Document Scanning Service to facilitate the re-tender of both contracts.

Without the continuation of these services this would effectively bring our service to a hold and enforcement of parking within the borough will likely be severely affected.

Key stakeholders include; Parking Services, members, policy

Our intended recipients of services are; residents, businesses, members of the public

	PART ONE: INITIAL SCREENING				
	Question	Examples	Yes	No	Description (Mandatory) ***Please overwrite the guidance advice***
1.	Will your project include capturing any information about individuals that can identify them? .	Non-residential building project New Arboricultural Tree database New CCTV Boroughwide Service New Library System Extensive and expanded upgrade of an existing system	☒	☐	*If you answered **No**, please provide a brief description of why you believe no personal data will be processed. For example, will the information be wholly anonymised. The Information about Buildings or Businesses and not people. Then send this to the Information Management Team*

	PART ONE: SUPPLEMENTARY SCREENING QUESTIONS CHECKLIST TO DETERMINE IF A FULL DPIA NEEDS TO BE COMPLETED.

	Please answer all questions in this section. If you Ticked **Yes to question 1.** Answering Yes to any questions from 2-10, means you will need to complete Part Two	Examples	Yes	No	(**Guidance**) What are the likely Data Protection Considerations ***you*** will need further advice from the Information Management and Governance Team/DPO
2.	Are you seeking to obtain information directly from individuals	Names, addresses, DOB, ethnicity	x	☐	Privacy Notice
3.	Is the information you plan to collect likely to be shared?	Social services, debt advice, police, fraud prevention	x	☐	Data Sharing, Contracts, Sharing Agreements
4.	Have you identified the source of the data	Council Department; Partner Agency; Contractor; Data Subject	x	☐	Data Flows, Contracts, Sharing Agreements
5.	Do any of the processes you are proposing to use include automated decisions making.	Automatically sending out letters to tenants in arrears without a manual check.	x	☐	Data Protection by Default and Design
6.	Are you planning to undertake any profiling of individuals, data matching or use of algorithms (AI) to track, monitor or profile individuals.	Targeting people based on profiling data such as age, ethnicity or religion for services and goods. Or Use of data warehouse for determining fraudulent housing benefit claims	☐	x	Rights and Freedoms of Data Subjects. And Data Storage and Retention Lawful Basis
7.	Personal data will be processed in a way which involves tracking individuals' online or offline location or behaviour.	Lone worker devices, cookies, google analytics; self-service online tools	☐	x	Refer to Council Guidance on use of New Technologies, council's privacy statement, and Appropriate Policy
8.	Will your project include processing Child Data.	Tenancy household composition or specifically aimed at children where you will offer goods or services	☐	x	Targeted processing may require compliance with the Children's Code. Consult IM team

9.	Will your project include the use of CCTV and/or other recording will be used	Recorded images or video will be captured, which may include identifiable images of people.	x	☐	Privacy Notice, Lawful Basis, Data Retention and Storage. Contract
10.	Could the data you plan to process involve highly sensitive information, such as women's refuge addresses, whistle blowing, vulnerable adults etc	Domestic violence, people flagged as a high risk to staff or other customers.	☐	x	*Other types of sensitive data refer to ethnicity/race, health, sexual life/orientation, religious affiliation, political opinions, trade union membership, genetic and biometric data*

Recommendation	
Is a DPIA required? If **Yes,** go to Part Two	Yes ☒ No ☐
If **No**, obtain sign off from the IM Team and place a copy on the project file If **No**, Note the Date Completed Obtain IMT Sign Off	

PART TWO

PART TWO: **DATA PROTECTION IMPACT CHECKLIST**			
Part Two is to be completed if you answered **Yes** to *any* section of Part One: DPIA Screening. Part Two is intended as a guide to help you identify how your project or initiative will engage the UK GDPR and Data Protection Act 2018. This will then enable you to complete Part Three (sections 1, 2 and 3) the Risk Assessment, i.e., the risks and issues associated with your proposed processing of personal data. P**lease** complete the Part Two Checklist by answering all the questions. Ignore column 1 which is for official use by the Information Management Team. Column 3 **Issues to Consider** is aimed at you whilst GDPR Considerations in Column 4 is aimed at the IM Team, but you can also consider them in your response.			
IM Team Only	Question	Issues to Consider	Response (**Mandatory**) You must provide an answer and can overwrite any guidance provided in this column

1.	Please Explain the purpose of the project, what it aims to achieve and what type of processing it involves (data handling).	*You may find it helpful to refer or **link to** other documents, such as **a project proposal brief or PID.***	Direct award for 2 key parking contracts; 1) Statutory Document printing contract – printing of keeper details including; Name/Company, address, vehicle registration number, PCN number, location/date/time of contravention. 2) Scanning and remittance processing contract – Scanning of customer written challenges & representations against PCNs as well as cheque payments. Service provider will scan all correspondence and allocate to the respective PCN case.
2.	Please describe the data that you will be processing. Including whether the data subjects are tenants, service users, Council employees etc.	***List sets of data** rather than individual fields, e.g., customer names, contact details, including telephone number and email. Are you planning on collecting information about, household members, addresses, profiling data, arrears data, and repairs history.*	Data subjects include; • Residents • Businesses • Member of the public Data we will be processing will include; • Customer name • Customer address • Customer contact details • Vehicle Registration Mark • PCN No. • Customer evidence (including medical documents, disabled badges, Police confidential paperwork) The Data Controller will be the Council and currently adhere to council security and data policies. We also have data sharing agreements in place with both contractors for each contract.
3.	Is the Council the Data Controller, the Data Processor, or a Joint-Controller? For advice on what these roles mean see here	***Who will control the data** – your team, jointly with a partner organisation/service, or will you be commissioning this work, Please see guidance on Information Sharing.*	RBKC – Parking Services are the data controller Capita – data processor Paragon – data processor

4.	How many individuals' data do you envisage the project will process.	**Larger datasets/bases** usually **pose more risk.** However, it is important to understand the scope of your project in terms of numbers as this has implications for the UK GDPR	In a yearly period we send out approx. 44,500 Notice to Owner statutory documents and 33,600 Moving Postal PCN statutory documents. Further statutory documents will be sent to the same individual if they do not pay or challenge the PCN. In a yearly period we will receive approx. 13,000 written PCN challenges/representations and 1,219 cheque payments for the scanning and remittance service.
5.	What is the lawful basis for processing the data? (see guidance) For example, tenancy agreement, lease, contract, specific consent.	**Is there a statutory, regulatory, or official reason underpinning your project,** which explains why you need to collect this information? It could be either direct, e.g., there is a legal obligation (homeless application) or indirect, e.g., the council has the power to undertake this project, even though there is no specific statutory obligation (customer satisfaction surveys, marketing council services, undertaking community consultations).	Yes – there is a statutory/regulatory reason underpinning this project. Both contracts are governed by The Traffic Management Act (TMA) 2004. • The Statutory document printing Contract is in place to enable the enforcement of PCNs under the TMA 2004. • The Statutory Scanning and remittance contract is in place to enable customers to challenge or pay a PCN under the TMA 2004.
6.	What is the source of the data?	Examples include the customer themselves, a representative of the customer, another organisation e.g., NHS partners, voluntary sector etc. Or another WCC/RBKC department. List all that apply.	• Customers • Representatives of the customer • DVLA • Enforcement Agents (Marston & Newlyn)
7.	If you already have access to the source of data, are you planning to use it in a different way when compared to why it was first collected?	**Does your service own the data?** If yes, are you planning to use it in a new way which is distinct from the original reason for collecting it? If your service **does not own the data**, where do you intend to source the data from and will you be using it for a different purpose compared to why it was first collected?	Parking Services owns the data. We are not planning on using it in a new way from the original reason.

8.	Does the data / processing include any of the following categories of data? If yes, please indicate which ones and provide a justification for processing /using the data: • Other household members or named individuals • Named children • Health & medical information including vulnerability • Race and ethnic origin; • Politics and trade union membership • religion; • genetics & biometrics (where used for ID purposes); • health; • sex life or sexual orientation.	*If you collect any of these categories, you must take extra care when processing this data.* *You cannot collect this data now for a potential unplanned future use!* *If you are going to collect any data highlighted in blue, this is legally classed as special category personal data, and you should address any risks this may pose under No.8 of the privacy risk assessment below.* *Go online to view the Appropriate Policy which sets out the council's commitment to processing Special Category aka Sensitive data* *Consider whether all the data items specified are required for the processing? Can any be removed, but still achieve the same ends?*	List of all data types the that will be processed • Customer name • Customer address • Customer contact details • Vehicle Registration Mark • PCN No. • Cheque details • Additional customer evidence (including medical documents, disabled badges, Police confidential paperwork) All data listed is needed and cannot be achieved without capturing person identifiable information. After processing the data, if an individual has requested their name, address and evidence to be removed from our debt management system (Si-Dem). We have a function to redact this data from Si-Dem.
9.	Is there another way of achieving the same project outcomes that does not involve processing individuals' data? What other options have you considered?	*This is to ensure that the scope of the project and data processing is in proportion with the expected outcomes.* *Consider whether any data items can be removed, but still achieve the same ends.*	No – this is a statutory requirement.

10.	Are you planning to issue, or have you already issued, a privacy notice to the world at large and/or your data subjects?	*Have data subjects been informed about this new processing, and any third parties that will have access to their personal data?* *If not at this stage, are their plans to ensure data subjects are informed either by you or your contractor/partner.*	A Privacy Notice has already been issued. This is printed on the physical copy of the PCN as well as the statutory document for Moving Postal PCN. This is also displayed on the RBKC webpage.
11.	What processes do you propose to put in place to ensure the continued accuracy of the data you plan to use? If you have already worked with the data describe how you verified its accuracy.	*Reasonable steps must be in place to ensure that data is accurate and kept up to date. Explain how your proposal will maintain accuracy for example capturing changes in customer information either using an API plugin or a manual update etc.*	Data received will either be from the customer directly or DVLA so data should be accurate from source. Where we are informed or it has been identified, the DVLA data and customer evidence can be redacted from the hosted debt management system (Si-Dem).
12.	Who will you be sharing data with, and how will you be sharing the data? Will the data ever be moved or stored outside of the UK?	*Do you know or have an idea about who you will be sharing data with, why and for how long? If you do know, please identify them in your response. This can include internal departments as well as external agencies.* *Examples of data sharing mechanisms include, automated data extracts, data manually uploaded onto an external website, emails to the organisation, posted forms or other documents.* *Consider whether data sharing is compliant and secure as part of your risk assessment.*	The data will be shared with Paragon via our hosted debt management system (Si-Dem). The dedicated operators working on this contract have been issued with a secure login and password. Data from DVLA is indirectly shared through the printing of statutory documents to Capita via a SFTP file. Only the required data fields are transferred. There are GDPR addendums to both contracts that deal generally with security. The data will not ever be moved or stored outside of the UK. There is an automated data extract applied to our hosted debt management system (Si-Dem), to write of and redact data after a period of 6 years. This is inline with statutory requirements.

13.	How is the data received? If you are planning to receive or share data have you completed the Third Party Information Assurance Form and had it reviewed.	*Examples of potentially non-secure data collection include, paper forms, unencrypted devices, non-secure email, use of fax machines.*	Data is sent to our statutory document printing contractor via an encrypted SFTP process. RBKC Data Retention period for Capita has been set as 2 years for scanned images. All PDF's are uploaded to EDMS system for PDF retrieval by RBKC. Data is not sent/received in any non-secure forms from any party.
14.	If you know provide details on where the data will be physically stored and/or processed	*Please list all relevant systems, business applications (e.g., IDOX, network drives (J: Q), hosted storage (e.g., case management provider); lockable filing cabinets.* *Please identify exactly where the information will be held on the world wide web such as UK, EU or Other. Consult IT if the data is likely to be stored outside the UK.*	The data will be physically stored and/or processed on our hosted debt management system (Si-Dem). All data is held within the UK. Capita process the data in Mansfield and physically print out statutory documents that are then securely collected by Royal Mail to be posted to the keeper of the vehicle.
15.	Who will have access to the data? How will you ensure that access is restricted to essential users?	*Data must be protected to prevent unauthorised or unlawful processing.* *Please specify teams, job roles and include external organisations. In some cases, this may be named officers.* *For example, you plan to restrict access to a SharePoint site to named users; or you are going to create role based accounts that will define and limit access.*	Data will be restricted on the hosted debt management system (Si-Dem) to authorised users issued with a secure login and password. *Who can access the data;* • *RBKC - Parking Operations, Fraud team, Customer access* • *Trellint (parking system provider)* • *Capita (process statutory letters)* • *Paragon – (lookup facility to the parking system to support the scanning of incoming correspondence and the processing of cheque payments)* • *Enforcement Agents (Marstons Group Ltd) and (Newlyn Plc)* • *NSL (enforcement provider) supervisors, team leaders and managers*

16.	How will you ensure that the data will be retained in line with the Corporate Data /Retention Policy and Schedule	Allocating time for how long your service records should be kept amounts to having a retention schedule. All council data should have a retention period, including those held in electronic as well as manual form, regardless of where they are stored. ***Contractors and Partners:*** *Ensure you have an exit strategy built it to any contractual or information sharing agreements so that you know exactly what will happen to the council's data at the end of the project/contract or information sharing arrangement*	The PCN data is governed in line with legislation and kept for a period of 6 years. RBKC Data Retention period for Capita has been set as 2 years for scanned images. All PDF's are uploaded to EDMS system for PDF retrieval by RBKC. Paragon – Currently keep RBKC documents on-site for a month and then the documents are moved to an off-site storage unit where they are stored for 12 months before being securely destroyed.

Risk Rag (Official use only for IM team to review and grade)

Risks are relatively insignificant or minor and can be readily addressed	Risks are moderate and will require a little more effort to fix, but is not a showstopper	Risks are potentially damaging to both individuals and the council and will require active resolution	Major potential risk that could be a showstopper and require active engagement to avoid.

PART THREE

Section 1. Guidance on how to complete Part 3

- We have provided pre-populated data protection privacy risk questions which you need to address. These are based on the data protection principles under UK GDPR and DPA 2018. If you identify other risks, you can add more risks under the **Additional Risks** category.
- It is important you capture what actions you will take to reduce any identified risks to the processing of personal data. Always think of the worst case scenario and then work back on what measures could be put in place at any point in the processing (start, middle or on-going) to either prevent or reduce high risk.

- If there is nothing that can be done to mitigate high risk the council is obliged to consider consulting the Information Commissioner's Office [ICO] **before** proceeding with implementing the project. Please consult the council's DPO if this is the case.

HOW TO COMPLETE THE RISK RATING ASSESSMENT TO GET A SCORE

1. Use the tables for 'Description of likelihood ratings' and 'Description of impact ratings' to objectively select and score the respective impact and likelihood ratings of each identified risk
2. Record your scores in the relevant column in Section 2 Privacy Risk Assessment
3. Multiply the respective scores for impact and likelihood to arrive at a risk rating score for each identified risk.
4. Document the risk rating score in the appropriate column
5. Identify the controls/measures/actions you need to put in place for each risk and document them in the Mitigations column to correspond to the risk they are designed to address to assist the risks areas have already been ragged (see below)
6. At the end, sum up the total scores in each column and find the average of the scores for each i.e., add up all scores and divide by the number of entries for each column.
7. Once your DPIA is complete please send to the IM team or if you work in ASC/ChS/PH ensure you also send a copy to with the IG/Caldicott Support Manager to discuss. Where you have answered "no" to all the screening questions, we still advise you contact the IM team to confirm your score.
8. A record of your DPIA and score will be registered on the council's DPIA register managed by the council's Data Protection Officer [DPO] and IM Team

UNDERSTANDING DATA PROTECTION RISK

This section follows up on the answers you've provided in sections 1 and 2 of the DPIA. In this section you need to assess the information (data privacy) risks that relate to the intended processing of personal data. In doing so you need to identify and assess **how the possible misuse of personal data could lead to significant impacts on:**

- Individuals (data subjects such as our service users, residents, staff etc.) - because their rights under data protection law are breached e.g., someone accesses their data who should not. Or our poor record keeping means we are unable to find their information when they ask for it.
- The service/the council - because our processing doesn't comply with the law – e.g., we sent out a spreadsheet containing a 150 names and other information about clients to the wrong email address. This is a data breach which is potentially reportable to the ICO and could result in a fine.

- A **risk** is something that may occur
- An **issue** is something that has occurred
- In calculating risk, there are two components you need to consider: *Risk = Likelihood * Impact*:
  - the **likelihood** of a risk materialising to become an issue (something that has happened = probability)
  - the **impact** that will be felt if the risk were to occur
- **Risk Rating** – when the impact (i) and likelihood scores are times together = Risk Rating

MITIGATION

Finally, to avoid or limit the impact, we need to think about what actions (**mitigations**) we can take to manage or plan, for the future.

- A **mitigation** is a control, measure, action we can take to either stop/reduce the likelihood of the risk occurring or reduce the impact if the risk does occur (i.e., if the risk becomes an issue).

MATRIX Using Impact and Likelihood Rating to Assess Data Privacy

RISK FORMULA: RISK = LIKELIHOOD * IMPACT (please see section 1 Guidance on How to Complete this section)	
DESCRIPTION OF IMPACT RATINGS (Risk Impact) Use these categories when determining the nature of the impact	**DESCRIPTION OF LIKELIHOOD RATINGS (Risk Probability)**
IMPACT	**LIKELIHOOD**

Impact	Descriptions
1. Insignificant	Insignificant impact to the individual or the Council Will not harm the individual, their property or livelihood. No reputational or financial loss to the council.
2. Minor	Minor impact to the individual, service, or the Council. Seen as an inconvenience, requiring short term recovery. Small number of individuals could be affected. Costs to the council considered low. The information is not biographical or does not include special category personal data. But does not engage with data subject rights, for example by having a Privacy Notice
3. Moderate	Moderate impact to the individual, service, or the Council. Not life threatening but will cause some inconvenience to the individual. Short to medium term recovery. Unauthorised access to, loss or damage to sensitive data of 11-999 individuals, cost impact could be significant to rectify
4. Major	Major impact to the individual, service, or the Council, Decrease in perception of public standing at regional level – regional media coverage, medium term recovery from incident. Unauthorised access to, loss or damage of sensitive data. May reach reporting to ICO threshold
5. Catastrophic	Catastrophic impact to the individual, community of users, or the Council. For instance, Life or Death situation, shut down in service for more than 1 days – for example inability to access social care systems. Will require reporting to the ICO

Descriptor	Likelihood Guide	Mitigations *Mandatory*
1. **Rare**	Virtually impossible to occur 0 to 5% chance of occurrence.	
2. **Unlikely**	Very unlikely to occur 6 to 20% chance of occurrence	
3. **Possible**	Likely to occur 21 to 50% chance of occurrence	**Possible** and **Probable** require you to outline the type of measures that could or will be taken to mitigate the risk
4. **Probable**	More likely to occur than not 51% to 80% chance of occurrence	
5. **Almost Certain**	Almost certain to occur 81% to 100% chance of occurrence	

Section 2: The Privacy Risk Assessment: Identify all Possible Risks (Likelihood and Impact) Arising from your proposed use of Personal Data. Please Complete this section. If you have answers you can overwrite the Appropriate Mitigation Controls

Privacy Risks	Like-li-hood (l)	Impact (i)	Risk Rating l times i = RR	Appropriate Mitigation Controls you will put in place (ignore the Rag as this will be applied upon review by the IM team)
1. Your description of the purpose of the project, what it aims to achieve and who the key stakeholders (internal or external) are ill defined.	1	3	3	Description of the project is clearly defined along with key stakeholders.
2. You have not or cannot list all the data items you plan to capture.	1	3	3	*All data items listed*
3. You have yet to decide who will control the data you intend to process, either singularly or jointly with a partner organisation/service, under a contract.	1	3	3	*This is clearly defined*
4. You do not know/understand the size or number of individuals who will be impacted by your project/procurement	1	3	3	*This is clearly defined*
5. At this stage you do not have a clearly defined legal basis for proceeding personal data or special category data aka sensitive data	1	3	3	*This is clearly defined*
6. You are unclear about the source of the data and have no agreements or structures in place	1	3	3	*This is clearly defined*
7. You can identify the source of the data but remain unclear about the controls you need to have in place to use it, such as anonymising it, ensuring that service users are made aware (now on in the immediate future) about the change in use	1	3	3	*This is clearly defined*
8.You are unclear about why you want to collect each of the personal data items you have mentioned, and why you wish to collect special category data.	1	3	3	*This is clearly defined*
9. You do not seem to have considered and dismissed a legitimate alternative means for collecting the information without having to identify individuals	1	3	3	*This is clearly defined*
10. You do not have a valid communication strategy to ensure users understand how their data will be used	1	3	3	*This is clearly defined*
11. How will you remove the possibility of "garbage in garbage out" to ensure up to date and accurate data	2	3	6	*If the data is inaccurate and is the* customer *who has provided the inaccurate data. They will be advised we need accurate*

				data if we are aware of this. If the DVLA has provided inaccurate data there is no recourse for this.
12. You are unclear about who you will share the data with and what kind of governance controls you need to put in place.	1	3	3	*This is clearly defined*
12a. You are unclear about what IT controls you will need to put in place, including any you will require a potential contractor or partner to have	1	3	3	*State here how you will resolve or mitigate this risk – Project Design Issue. Use of IS Third Party Questionnaire*
12b. You have not considered the impact of data being processed outside the UK? If you have considered it, what controls will you put in place so that you understand where council data will be located at any given point in time	1	3	3	*This is clearly defined*
13. You have not considered the security controls needed to protect the data you receive, store, or send.	1	3	3	*This is clearly defined*
I4. You have not sufficiently mapped where the data will be held internally	1	3	3	*This is clearly defined*
14a. You have not considered the data flow requirements and how these will be managed.	1	3	3	*This is clearly defined*
15. You have not envisaged or crafted details about what the access controls should be for the type of data you intend/are processing.	1	3	3	*This is clearly defined*
15a You have not considered how you build audit capabilities (technical or operational) into your solution to guarantee you can identify how data has been accessed and used.	1	3	3	*This is clearly defined*
16. You are unfamiliar with the council's records retention policy and schedule, and have not scoped data retention into your solution design	1	3	3	*This is clearly defined*
Additional Risks				
INITIAL SCORE			63	

Next: Once completed consult the Information Management Team – who will review your initial score, then agree with you a final score

IM/IS ONLY Recommended Actions (tick) Nature of Mitigation			
	Early Risk Remedial Action		Project Design Issue
	Scoping Issue		Critical Issue

Once completed contact the IM Team to review and assess with you your answers. A final score will be provided, and you must then take the appropriate action to obtain sign off for the DPIA as set out below.

	Immediate IM/IS Recommended Action	**Date Implemented**
1		
2		
3		

FINAL AGREED PROJECT RISK RATING (TICK RELEVANT BOX)	
Risk level	**Agreed Outcome: Closed. Open and under Review**
Low 1-10 - Project can proceed	
Medium 11-15 – Recommend minor actions are required before proceeding	
High 16+ - Recommend significant actions required before proceeding	
FINAL SCORE …….	

Section 3. Risk Tolerance

If any of the captured mitigations and IM recommended actions will not be implemented, then the signatory must capture this here and by signing confirm they accept the additional risk posed by the rejection.

I agree not to implement the following IM recommendations (list below)

Signature_____

Date_____

Section 4. SIGNATORIES

This DPIA must be signed off by the project sponsor or information asset owner. The SIRO should only be consulted where the risk rating is 16 or higher and will involve council IT network or infrastructure.

I am satisfied that this DPIA is an accurate summary of the intended processing of personal data, the related risks and the mitigations that will be adopted.

Name and Signature of Information Asset Owner (Mandatory)

Date

Name and Signature of Senior Information Risk (If consulted)

Andy Vennard
Head of Parking Services

Date 16/01/2025

APPENDIX 1

If during the project **new** processing is proposed and/or **risks** arise please complete the table below to document the Change Control and the steps taken to mitigate any identified risks.

DPIA Implementation and Change Control				
Risk	**Date**	**Nature of change**	**Person responsible [name and job role]**	**Action Taken**