Privacy Impact Assessment

Blue Badge

APPENDIX A

Privacy Impact Assessment – Screening Questions

Question	Y/N	Additional Comments (please give reasons for either a 'yes' or' no 'answer here)
Is there a requirement under GDPR to carry out a PIA? NB if there is a legal requirement to carry out a PIA there is no requirement to complete the remaining questions.	Y	
Will the project involve the collection of new information about individuals?	Y	
Will the project compel individuals to provide information about themselves?	Y	
Will information about individuals be disclosed to third party organisations or people?	Y	
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
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.	N	

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Y	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, health or information concerning an individual's sex life or sexual orientation or other information that people would consider to be private.	N	
Will the project require you to contact individuals in ways that they may find intrusive?	N	
Will the data be held in relation to children or vulnerable adults?	Y	

APPENDIX B

Privacy Impact Assessment

Step 1 – Requirement for PIA – issues to be addressed

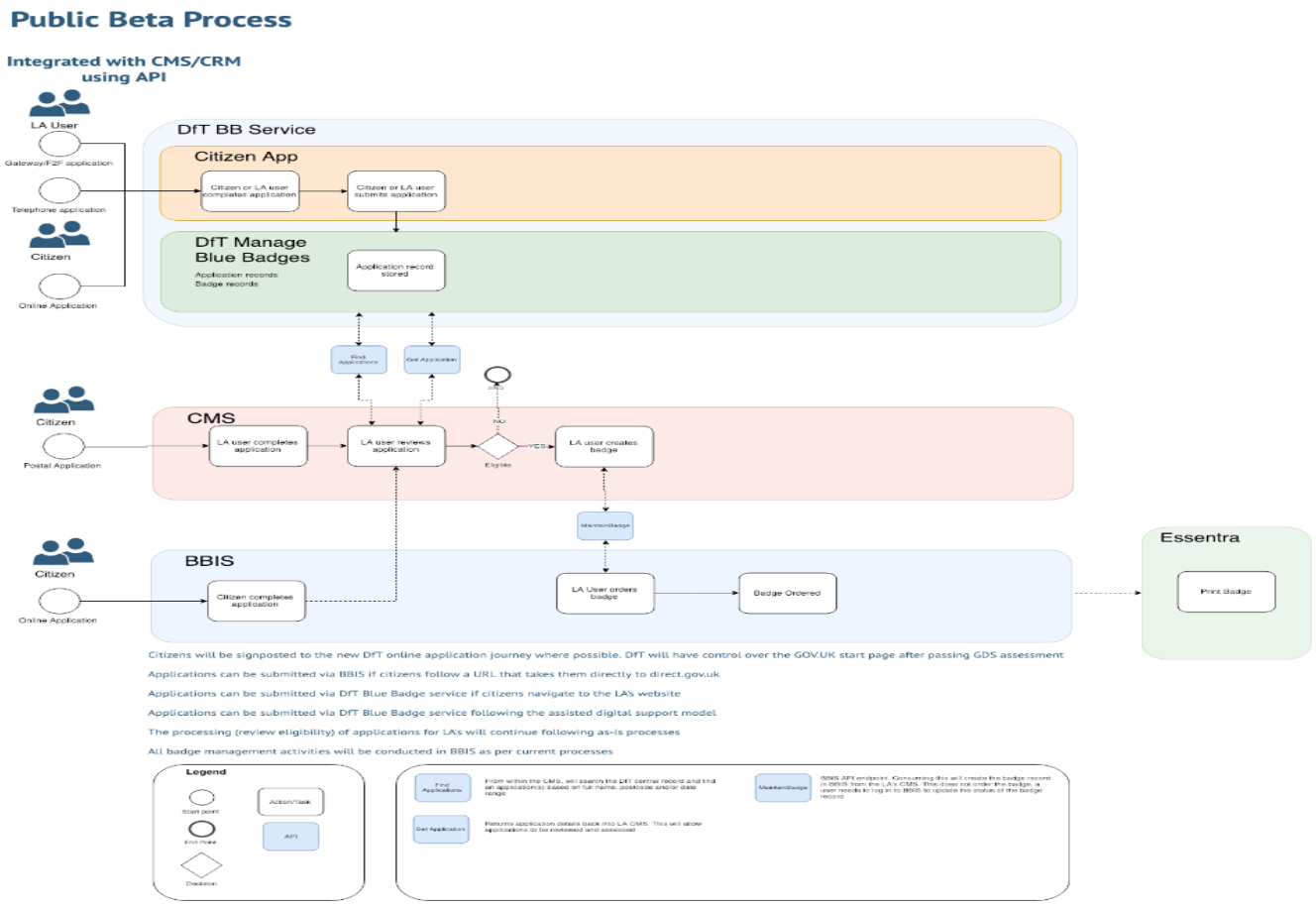
- Project Aim and Objectives
  - To administer blue badge applications on behalf of Derbyshire County Council
- Benefits to the organisation, to individuals and to other parties of personal data
  - To identify client journeys through the application process of applying for a blue badge
  - To enable citizens with disabilities and health issues to benefit from parking concessions
- Summary of Identified Need for PIA (can draw on answers to the screening questions)
- - Citizens apply for a blue badge by answering questions relating to their health. The authority uses this information to assess eligibility. If an application is approved then this information is transferred to a third party in order for the badge to be printed and distributed.

Step 2 – Information Flows/Nature of processing

- Description of collection, use, retention and deletion of personal data - is any sharing of data involved?
  - Yes - Applications are received by the authority through the post (paper), by e-mail and electronically from the national blue badge database. Following assessment, data is currently transferred to Northgate's BBIS system for printing and distribution of the blue badges. From 05/02/19 this system will be replaced by a new national system provided by Valtech UK who have been contracted the Department for Transport.
- Explanation of data flows – diagram or description detailing: controllers and processors, storage location and storage method, personal data fields collected, individual/team/organisational access to personal data(audit trail), security measures for storage and transfer of data
  - Derbyshire County Council blue badge administrators receive applications and input information into Derbyshire County Council's internal blue badge system. If the application meets eligibility criteria the information is transferred to the national blue badge system for distribution and posting.
- Number of individuals likely to be affected by the project - do they include children or other vulnerable groups?
  - Not really affected as the process for applying is the same as it is now. Approximately 18,000 badges are processed per year. All of the data is for any age of clients with regards to processing their blue badge application.

- Does the data include special category or criminal offence data? – No

The following diagram illustrates the flow of data:


Public Beta Process
Integrated with CMS/CRM using API
LA User
Gateway/F2F application
Telephone application
Citizen
Online Application
DfT BB Service
Citizen App
Citizen or LA user completes application
Citizen or LA user submits application
DfT Manage Blue Badges
Application records
Badge records
Application record stored
Find Applications
Get Application
Citizen
Postal Application
CMS
LA user completes application
LA user reviews application
Eligible
YES
NO
LA user creates badge
MaintainBadge
Citizen
Online Application
BBIS
Citizen completes application
LA User orders badge
Badge Ordered
Essentra
Print Badge
Citizens will be signposted to the new DfT online application journey where possible. DfT will have control over the GOV.UK start page after passing GDS assessment
Applications can be submitted via BBIS if citizens follow a URL that takes them directly to direct.gov.uk
Applications can be submitted via DfT Blue Badge service if citizens navigate to the LA's website
Applications can be submitted via DfT Blue Badge service following the assisted digital support model
The processing (review eligibility) of applications for LA's will continue following as-is processes
All badge management activities will be conducted in BBIS as per current processes
Legend
Start point
End Point
Decision
Action/Task
API
Find Applications
From within the CMS, will search the DfT central record and find an application(s) based on full name, postcode and/or date range
Get Application
Returns application details back into LA CMS. This will allow applications to be reviewed and assessed
MaintainBadge
BBIS API endpoint. Consuming this will create the badge record in BBIS from the LA's CMS. This does not order the badge, a user needs to log in to BBIS to update the status of the badge record

Step 2 – Consultation Requirements

Identify whether internal and/or external consultation is required to address privacy risks

- Stakeholders to be consulted – Not needed as there is no change for residents applying for a badge.
- Method of consultation – N/A

Part B Steps 3 to 4 – Identify Privacy Risks, Solutions and Approval

Privacy Risk	Risk to Individuals & organisation	Risk initial score	Action Identified	Target Score (after applying actions)	Risk Control Plan (Treat/Control/Tolerate/Accept/Terminate/Transfer)	Evaluation: is the final impact on individuals and the organisation after implementing each solution a justified, compliant and proportionate response to the aims of the project?	Approved By
Disclosure of the personal and sensitive data that is required for delivery of the service	Harm and distress if released, unauthorised access, or used for different purposes Inappropriate/excessive disclosure of personal and sensitive data	8	Access to the system will be limited to only those with the correct role based access activity. The use of the system will be managed locally through relevant training and guidance.	4	Control/Accept	Yes, the benefits of sharing the information greatly outweigh the privacy risk with the appropriate mitigation in place	
Retention schedule is not adhered to.	Data is kept longer than agreed	4	Retention schedule is in place. Any data that has met	2	Control/Accept	Yes.	

			the retention expiry date will be deleted.				

Step four: 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
Ensure that existing data privacy controls continue	Ongoing	Patrick Kerr

Contact point for future privacy concerns – Patrick Kerr x31312
Date of consideration by IGG

APPENDIX C

Linking the PIA to the GDPR 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 GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully

There must be lawful basis for processing the personal data as follows;

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

- Have you identified the purpose of the project and which lawful basis applies? | Y

- Is the processing of the data necessary in terms of GDPR? | Y

- How will you tell individuals about the use of their personal data?

There is a statement on the bottom of an application form informing what we as an authority will do to protect their data and how we use it.

- Do you need to amend your privacy notices? | N

- 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

- If special categories of personal data have been identified have the requirements of GDPR been met? | N/A

As the Council subject to the Human Rights Act, you also will where privacy risk are especially high need to consider:

- Will your actions interfere with the right to privacy under Article 8? N
- Have you identified the social need and aims of the project? Y
- Are your actions a proportionate response to the social need? Y

Principle 2

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

- Does your project plan cover all of the purposes for processing personal data? Y
- Have you identified potential new purposes as the scope of the project expands? N/A
- Does your Privacy Notice cover all potential users? Y

Principle 3

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

- Is the quality of the information good enough for the purposes it is used? Y
- Which personal data could you not use, without compromising the needs of the project?

The data collected is only what is required to process an application for a blue badge

Principle 4

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

- If you are procuring new software does it allow you to amend data when necessary? N/A
- How are you ensuring that personal data obtained from individuals or other organisations is accurate? An individual signs an application form to agree the information they are supplying is accurate.

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

- What retention periods are suitable for the personal data you will be processing?

3 years which is the length of time of a blue badge

- Are you procuring software that will allow you to delete information in line with your retention periods? | N

Principle 6

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

- Will the systems you are putting in place allow you to respond to subject access requests more easily? | N
- Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten). | Y
- If the project involves marketing, have you got a procedure for individuals to opt in to 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.

- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?

No training necessary as processing blue badges is the same

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.

- Will the project require you to transfer data outside of the EEA?
- If you will be making transfers, how will you ensure that the data is adequately protected?