Appendix 2 - Tri-Borough Privacy Impact Assessment

Section 1 - Assessment Details

1.1	**Title of Project/Programme/Process**	Improvements to Frank Banfield park, including the creation of a community garden
1.2	**Date of Completion of form**	12.12.18
1.3	**Name of person completing form**	Heather Marsh
1.4	**Your job title**	Parks Projects officer
1.5	**Your telephone number**	07468 711527
1.6	**Your directorate**	Residents Services
1.7	**Your Business Unit**	Leisure and Parks
1.8	**Your Team**	Parks Projects

1.9 What is the aim of the project, and what activities are involved?

Response:
The aim of this project is to improve amenities in Frank Banfield park, through installing new surfacing, planting and street furniture. A contract to carry out the works will be tendered using an open tender. The winning tenderer will be appointed and will carry out the landscaping works.

Guidance Note – 1.9
Please specify if this involves the procurement, commissioning or upgrade of a service or technology, or other

The more detail that is included in this section, the easier it will be to assess the impacts of the project. Outputs of the project must be clearly identified.

1.10 Initial Screening Questions

#	Question	Yes	No
1	Will the project involve the collection of new information about individuals?		N
2	Will the project compel individuals to provide information about themselves?		N
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		N
4	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
5	Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		N
6	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		N
7	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For nexample, health records, criminal records or other information that people would consider to be particularly private.		N
8	Will the project require you to contact individuals in ways which they may find intrusive?		N

Did you Answer **YES** to any of the above? If so Section 2 **MUST** be completed!

Completed By……Heather Marsh……
Position……Parks Projects officer……..
Signature……H J Marsh……
Date ……12.12.2018…….

Section 2 – Privacy Impact Assessment Checklist

2.1 Has a PIA/Checklist been undertaken for this initiative before? If so, please give dates and provide copy (where possible)

Response:

2.2 Please give details of any legal requirements for this project, e.g. government initiative, specific legislation for example: - Crime and Disorder Act 1998.

Response:

Guidance Note – 2.2
It is vital that any legislative requirement is outlined in this section; it will provide a strong support for the use of personal or sensitive personal data.

2.3 The project will use (process) the following data

Title of Dataset	**Data Source**		**Is the Data Sensitive Personal Data (Y/N)**
	Borough	**System**	

Guidance Note – 2.3
Please include all the data sets and their sources that will be used in the project. Even though some sources may not contain personal data, when combined with other data sets used these may create a new data set that will enable an individual to be identified.

Where the data used is either from CHS or ASC, the appropriate Caldicott Guardian must be consulted.

NOTE: For definitions of personal and sensitive personal data please refer to glossary at the end of the document.

2.4 How will that data be used and have the subjects of that data been informed of and/or provided consent for this purpose?

Title of Dataset	**Metadata Element**	**Reason for use of Data**	**Has consent been obtained for use (Y/N)**

Guidance Note – 2.4

Any use (processing) of personal data has to be undertaken in a fair and lawful way. Data used must also be relevant and not excessive. Therefore the project must be able to demonstrate exactly why the use of a data set is important.

Note: this cannot be just a "fishing" exercise

Obtaining informed consent from the individual to use their data for the specific purpose will provide a robust legitimate reason for using the data. Not having consent does not prevent the use of data, but you should consult with your local information manager if you are seeking to use data without consent.

Note: Metadata Elements are the individual data parts of a dataset, for example a dataset of client information may contain metadata elements such as "forename, Surname, Address, Age" each of which potentially could be extracted individually

2.5 Who do you intend to share the data with (name all intended internal and external recipients)?

Data Title	Who be given access to the data	reason for access

Guidance Note – 2.5
All data controllers must be able to trace when and where the data was collected and also who has been provided with access to the data.

2.6 When obtaining and/or sharing the data how will it be transferred? E.g. non-encrypted email, encrypted email etc.

Applicant response:

Guidance Note – 2.6
Personal data must be transferred in a safe and secure way. In this section you must outline the exact methodologies used in the project for moving/transferring data.

2.7 How will the data be stored, for how long will the data be stored, and what security arrangements are in place to maintain will exist in respect of the data?

Response:

Guidance Note – 2.7
Have you consulted / implemented where applicable, your borough's:

- Records Management Policy
- Retention Schedule

Information Security Standards:

- Have you consulted (and received sign-off from) the Information Security Manager (see contact details at end of this document)

2.8 What are the risks to the individuals whose data is being used in this project

Privacy Risks	Impact (i)	Likelihood (l)	Risk rating (i x l)	Mitigation
The data subjects (service users, customers, staff) have not been **notified of or consented to** (principle 1) this proposed **purpose** (principle 2) to process their personal and sensitive data. *[Insert the risk description here re: the principles 1 and 2 above or mark as N/A]*				*[Insert activities, controls or measures already established or planned – to help, ask yourself these questions: How will individuals be told about the use of their personal data? Do you need to amend privacy notices? Does your project clearly state it's purpose of using this information?]* • …
The personal and sensitive data sets to be handled are **adequate, relevant and not excessive (principle 3)** for the purposes of task in hand. *[Insert the risk description here re: the principles 3 above or mark as N/A]*				*[Insert activities, controls or measures already established or planned – to help, ask yourself these questions: is there any information you do not need access to? Are you collecting only the information you need?]* • …
The personal and sensitive data to be handled contains **inaccuracies (principle 4**) that will skew the accuracy of decisions taken. *[Insert the risk description here re:*				*[Insert activities, controls or measures already established or planned – to help, ask yourself these questions: How do you know the information you plan to use is accrate? How do you plan to maintain its accuracy?]* • …

the principles 4 above or mark as N/A]				
The personal and sensitive data handled is **retained** and destroyed **(principle 5).** *[Insert the risk description here re: the principles 5 above or mark as N/A]*				*[Insert activities, controls or measures already established or planned – to help, ask yourself these questions: What retention periods will be applied to the information before destruction? How will the information be destroyed at the end of the retention period?]* • …
The Personal and sensitive data should be processed in accordance with the **rights of data subjects.** There must be a documented process between the parties to ensure information requests are met. **(Principle 6).** *[Insert the risk description here re: the principles 6 above or mark as N/A]*				*[Insert activities, controls or measures already established or planned – to help, ask yourself these questions: How will this information be quickly accessed/blocked in a timely response to a subject access request, court order or litigation hold?]* • …
The personal and sensitive data is either **lost or unlawfully disclosed (principle 7)**. *[Insert the risk description here re: the principles 7 above or mark as N/A]*				*[Insert activities, controls or measures already established or planned – to help, ask yourself these questions: How are you protecting information (soft and hard copy) when being moved/transferred/migrated? What controls do you have to prevent unauthorised access/modification/disclosure?]* • …
The personal and sensitive data will be **stored** securely which is within the EEA **(principle 8)**. *[Insert the risk description here re:*				*[Insert activities, controls or measures already established or planned – to help, ask yourself these questions: Will the information be stored on systems held outside of the EU/EEA or the USA's Privacy Shield]*

the principles 8 above or mark as N/A]				• …
Overall				

Guidance Note - 2.8
The PIA process is a risk based model the aim is to identify any risks that may result for the use of personal data. The misuse of personal data could lead to significant impacts on the lives of individuals therefore prior to using any personal data all risks must be identified and mitigated.

In order to measure the correct level of risk you are required to assess this using the following risk methodology to determine the overall impact to your service or the Council.

Impact	Description
1. **Very Low**	• Insignificant impact to the service or the Council • Unauthorised access to, loss or damage to ordinary personal data of up to 10 living individuals, cost impact £0 to £25,000
2. **Low**	• Minor impact to the service or the Council • Localised decrease in perception within service area – limited local media attention, short term recovery • Unauthorised access to, loss or damage to ordinary personal data of 11-999 individuals, cost impact £25,001 to £100,000
3. **Medium**	• Moderate impact to the service or the Council • Decrease in perception of public standing at local level – media attention highlights failure and is front page news, short to medium term recovery • Unauthorised access to, loss or damage to sensitive data of 11-999 individuals , cost impact £100,001 to £400,000
4. **High**	• Major impact to the 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 to over 1000 individuals, cost £400,001 to £800,000
5. **Very High**	• Catastrophic impact to the service or the Council • Decrease in perception of public standing nationally and at Central Government – national media coverage, long term recovery from incident • Significant long term damage or distress to large numbers of people, cost £400,001 to £800,000.

Descriptor	Likelihood Guide
1. **Improbable, extremely unlikely**	• Virtually impossible to occur 0 to 5% chance of occurrence.
2. **Remote possibility**	• Very unlikely to occur 6 to 20% chance of occurrence
3. **Occasional**	• Likely to occur 21 to 50% chance of occurrence
4. **Probable**	• More likely to occur than not 51% to 80% chance of occurrence
5. **Likely**	• Almost certain to occur 81% to 100% chance of occurrence

Mitigations
You are required to outline of any mitigating measures that have been taken as part of the project to help justify the score given.

Note: This risk may be subject to moderation following the review by the information managers

2.9 Will the project involve any surveillance of any person by any means? (e.g. CCTV, communications monitoring)

Response:

2.10 Will the project involve any targeted marketing activities? For example: the promotions of goods or services via post, telephone and/or email?

Response:

Guidance Note – 2.10
Any targeted marketing activities will require consent of the data subject. This should if possible be explicit consent and evidenced as part of the completion of this process.

If explicit consent has not been provided then it may be possible to imply consent however to determine this you should consult with your local information Manager.

2.11 At what stage in the project are you completing this checklist and what is the target deadline for "go live"?

Response:

2.12 Have you or do you plan to include data protection in any of the governance documentation, such as requirements specifications, contracts, risk and issue logs or SLA?

Response:

2.13 Do you plan to use live personal data in testing the new system?

Response:

2.14 Where will the shared data be held/stored?

Response:

Project Manager Name……...

Project Manager Signature……

Date……..

Section 3 – Information Management Review (this is to be completed by the information managers)

3.1 Comments

IM Comments:	
H&F	The content of this PIA has been evaluated reflects that there are no personal data processing involved in this project therefore there are no data provacy risks to be evaluated Christopher Ndubuisi Senior Information Management Officer London Borough of Hameersmith and Fulham
RBKC	
WCC	

3.2 Required Actions

#	IM Requirement	Date Met
1		
2		
3		

3.3 Final Agreed Project Risk Rating (Tick relevant box)

Risk level	
Low 1-10 - Project can proceed	
Medium 11-15 - Minor actions are required before proceeding	
High 16+ - Significant actions required	

3.4 Sign off Level – Recommendation

Following the review of this PIA the Information Manager/s recommend that this PIA is signed off by

Tick Box	Level
	Senior Information Risk Owner (risk level 16+)
	Information Manager (risk level 11-15)
	Information Asset Owner (risk level 1-10)

Section 4. Signatories

Signature of Information Asset Owner……..

Signature of Information Manager……..

Signature of Senior Information Risk Owner……...

Print Name of signatory……

Date……

Section 5 - Key Contacts

Information Managers		
Name	**Council**	**Email Address**
Ciara Shimidzu	LBHF	Ciara.Shimidzu@lbhf.gov.uk
Fatima Zohra	WCC	fzohra@westminster.gov.uk
Liz Man	RBKC	Liz.Man@rbkc.gov.uk
Information Security Managers		
Name	**Council**	**Email Address**
Adrian Dewey	LBHF	Adrian.Dewey@hfbp.co.uk
Phil Catling	WCC	pcatling@westminster.gov.uk
Valerie Benmehirize	RBKC	Valerie.Benmehirize@rbkc.gov.uk

Glossary

<To Be Added>