Appendix 6

Tri-Borough Privacy Impact Assessment Template

1. What Is a Privacy Impact Assessment (PIA)?

A privacy impact assessment is a simple, risk based mechanism to help identify the potential level of risk when undertaking a project involving the use of personal data.

2. When Is a PIA required?

At the point where any process, programme or project brief is being created it must be risk assessed using a PIA. The PIA must be undertaken at the point a business case is being devised, prior to the Project Initiation phase. This ensures the risks are fully understood and can be integrated when assessing the viability of the project, as the costs of mitigating the risks may be too great.

3. Completing the PIA

Each section of the PIA is to be completed as fully as possible - the more information that is provided, the easier it is to ensure the risks properly assessed. If a question or section is not relevant to your project then it should be indicated as N/A (Not Applicable).

Each section of this template has been created to make things as straightforward as possible, with specific guidance notes in place. Prior to completing this PIA you should familiarise yourself with the Information requirements, policies and guidelines of you local borough:

City of Westminster – Knowledge and Information Management
Hammersmith & Fulham – Information Management
Royal Borough of Kensington and Chelsea – Information Management

If you have any further questions please contact your local Information Manager (contact details at end of document).

4. Process For completion

a. The Project Manager/lead officer from the service to complete the PIA
   Section 1 – This provides an initial screen to identify those projects that do not require the completion of a full PIA.
   Section 2 – This section must be completed if any of the initial screening questions are **YES**

b. Send completed PIA to the Tri-borough Information Managers who will review and feedback.

c. Once the review process is completed send to the relevant Senior Information Risk Owner, Information Asset Owner or Information Manager for sign-off

d. Hold onto a copy of the signed PIA with the project documentation and also send a copy to your local Information Manager

DO NOT SUBMIT THIS COVER SHEET

Tri-Borough Privacy Impact Assessment

Section 1 - Assessment Details

1.1	**Title of Project/Programme/Process**	Procurement of MSP for Agency Workers
1.2	**Date of Completion of form**	29 December 2015
1.3	**Name of person completing form**	Gordon R Smith
1.4	**Your job title**	Shared Senior HR Business Partner
1.5	**Your telephone number**	020 8753 2958
1.6	**Your directorate**	FCS
1.7	**Your Business Unit**	Human Resources
1.8	**Your Team**	HR

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

Response:

The Council currently outsources the recruitment, management and payment of Agency Workers to a Managed Services Provider (MSP). The contract is due to terminate in June 2016 without the option for extension and it is necessary to ensure that a new MSP contract is procured timeously.

Agency Workers are not Council employees.

The cabinet report seeks permission to procure a new MSP contract direct via a national framework which will negate the need to go to tender.

Therefore no personal information is being used or stored to assist the Procurement Exercise.

However, the Contract to be procured relates to the recruitment of Agency Workers and therefore recruitment agencies will be required to obtain and share certain personal and screening recruitment information with Pertemps, BT (Agresso) and H & F to assist with eg selection processes, salary administration, record keeping and monitoring etc projects deemed necessary for the smooth running of the Contract.

The Contract will include reference and adhesion to all relevant aspects of the DPA and the Privacy of sensitive information by Pertemps and the c 67 recruitment agencies.

1 Approximately 67 Recruitment Agencies will ingather recuitment information submitted by job applicants and will also conduct screeneing for eg right to work, DBS etc
2 Recruitment information for selected candidates will be shared with H & F recruiting Managers who will make value judgements on candidates shared information.
3 Pertemps will hold relevant recruitment information on engaged agency workers and will share this with BT via an electronic interface established between PAWS (Pertemps Agency Workers System) and Agresso for finance, invoice and payment purposes. Candidate names will be visible on agresso
4 Pertemps will share engaged information with selected HR staff on request to assist with monitoring, future procurement, and other specific exercises.

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?	x	
2	Will the project compel individuals to provide information about themselves?	x	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		x
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?		x
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.		x
6	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		x
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.		x
8	Will the project require you to contact individuals in ways which they may find intrusive?		x

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

Completed By…………Gordon R Smith…………………………………
Position…………………Shared Senior HRBP…………………………..
Signature……………………………………………………………….
Date ……………….…30 December 2015……………………………..

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:
No

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:
N/A

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	
Recruitment and Personal Information	LBHF	PAWS / Agresso	Yes, in part

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)

Personal Records	All	Recruitment, Assessment and Payment and monitoring	Yes

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**
Personal Records	Recruitment Agency	Recommending Worker(s)
	Pertemps	Recruitment information for selected candidates will be shared with H & F recruiting Managers who will make value judgements on candidates shared information. Pertemps will hold relevant recruitment information on engaged agency workers and will share this with BT via an electronic interface established between PAWS (Pertemps Agency Workers System) and Agresso for finance, invoice and payment purposes. Candidate names will be visible on agresso
	BT (Agresso)	for finance, invoice and payment purposes. Candidate names will be visible on agresso
	H and F	Selection Decisions (Recruiting Manager)

		and HR Staff for with selected HR staff on request to assist with monitoring, future procurement, and other specific exercises.

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:
Electronic Transfer via password protected spreadsheets attached to emails

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: Within LBHF
Electronically in password protected desk top computers
Paper spreadsheets will be retained in locked drawers and / or cabinets
Both for the duration of the engagement or the exercise being conducted

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

Risk	**Impact (i)**	**Likelihood (l)**	**Risk rating (i x l)**	**Mitigation**
Public Access to personal records (Hacking)	**Low 2**	**Improbable 1**	**2x1 = 2**	**The Councils Firewalls to be relied upon**
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:
No

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:
No – for LBHF only occassional emails reminding of payroll deadlines or changes to deadlines

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:
At point of finalising report to Cabinet scheduled on 7 March 2016

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:
Yes – contract will include rweference to DPA and will reqwuire active adhesion to requirements

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

Response:

No

2.14 Where will the shared data be held/stored?

Response:

N/A

Project Manager Name…Gordon R Smith…………………………………………………………………...

Project Manager Signature…………………………………………………………………

Date…………30 December 2015…………………………………………………..

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

3.1 Comments

IM Comments:	
H&F	
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>