

Privacy Impact Assessment

Introduction

The Council handles information about individuals, such as residents, service users and its staff. A privacy impact assessment (PIA) is a process which helps the Council to assess privacy risks to individuals in the collection, use and disclosure of information. They help identify privacy risks, foresee problems and bring forward solutions.

Purpose

There are a number of reasons why the Council needs to conduct a PIA for its projects:

- To identify privacy risks to individuals
- To identify privacy and data protection liabilities for the Council
- To protect the Council's reputation
- To instil public trust and confidence in it's services and new projects

By conducting a PIA, the Council will identify and manage privacy risks appropriately whilst also understanding the type of information which is being included in projects.

Procedure

The first step in the process is to identify the need for a PIA. The screening questions are designed to help responsible officers to decide if a PIA is necessary and they are also designed to be used by project managers and other staff who are not familiar with data protection or privacy matters. The screening questions allow 'non-experts' to identify the need for a PIA as they are best placed within the Council to understand the types of information being processed.

For all new projects or changes in processes (or any activity which could have an impact on the privacy of individuals), the screening record form must be completed and signed off by the Chief Officer (or delegated officer) to show that the Council have considered the types of information being processed.

In some cases a PIA isn't required however justification for not completing the assessment must be recorded on the screening form as part of the audit trail.

Where the screening form indicates that a PIA should be completed, the template provides key privacy risks which the responsible officer will need to apply to the project/change in process and assess the risk as described in Appendix A of the template. It is usual for an officer involved with the project/change in process to complete the PIA however final sign off by the Chief Officer (or delegated officer) is required is required.

Definitions

A **Project** is a new project or any change in process regarding the handling of Personal Information; it includes obtaining, recording, holding/storing, disclosing, transmitting or disseminating personal information. Any activity which could have an impact on the privacy of individuals.

Personal Information is any information which relates to a living individual who can be identified – (a) from that information, or (b) from that information and other information which is in the possession of, or is likely to come into the possession of, the Council.

Sensitive personal information is personal information (as described above) consisting of information as to –

- a) the racial or ethnic origin of the data subject
- b) his/her political opinion
- c) his/her religious beliefs or other beliefs of a similar nature
- d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- e) his/her physical or mental health or condition
- f) his/her sexual life
- g) the commission or alleged commission by him/her of any offence, or
- h) any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings

VERSION	Version 3
DATE AGREED	November 2012
NEXT REVIEW DATE	November 2014
AGREED BY	Corporate Management Team
COVERAGE	This Procedure applies to Bracknell Forest Council
AUTHOR(S)	Information Management and Security Officer

Amendment to V1 – Penny O’Callaghan – reviewed and refreshed to take into account restructure December 2013

Amendment to V2 – Penny O’Callaghan – inclusion of risk column, rewording of some sections, Appendix A added and additional guidance April 2014

Screening Record Form for New Project / Change in Process / or any activity which could have an impact on the privacy of individuals

Date of Screening:	Directorate: Corporate Services	Section: Finance - Insurance
1. Project to be assessed	Retender of Casualty Insurance Programme	
2. Officer responsible for the screening	Helen Rogers	
3. What is the Project?	<input type="checkbox"/> Policy/strategy <input type="checkbox"/> Function/procedure <input type="checkbox"/> Project <input type="checkbox"/> Review <input checked="" type="checkbox"/> Service <input type="checkbox"/> Organisational change	
4. Is it a new or existing handling of Personal Information?	<input checked="" type="checkbox"/> New <input type="checkbox"/> Existing	
5. Personal Information involved	<input checked="" type="checkbox"/> Personal Information (information about an identifiable individual) See definitions <input checked="" type="checkbox"/> Sensitive Personal Information (such as health information or information about any offence) (*also tick Personal Information) See definitions <input type="checkbox"/> Over 1,000 records of Personal Information	
6. Type	<input checked="" type="checkbox"/> Collecting new Personal Information <input type="checkbox"/> Re-using existing Personal Information <input checked="" type="checkbox"/> Sharing Personal Information with another organisation <input type="checkbox"/> The project uses new or additional information technologies which have the potential for privacy intrusion	
	If two boxes are ticked at section 5 and one box at section 6 a full Privacy Impact Assessment should be undertaken.	
7. Summary of the business case justifying the Project	<p>The Council is retendering its liability insurance provider, including claims handling service. As part of the claims handling service the Council will receive personal information from members of the public who make a claim for compensation against the Council. Some of these claims will then be submitted to the Council's insurer or claims handling agents to investigate the claim.</p>	

8. On the basis of sections 5 and 6 above is a full impact assessment required?	Y	N	
9. If a full Privacy Impact Assessment is not required; what action will be taken to reduce and avoid privacy intrusion? Please complete the action plan in full, adding more rows as needed.			
Action	Timescale	Person Responsible	Milestone/Success Criteria
10. Chief Officer / Head of Service (or delegated officer's) signature.	Signature:		Date:

When complete please retain on the file and send a copy to Legal Services Penny.O'Callaghan@bracknell-forest.gov.uk.

Have you considered whether you need to do an Equality Impact Assessment?

Privacy Impact Assessment Template for New Project / Change in Process / or any activity which could have an impact on the privacy of individuals

The following should be completed and retained on the file with a copy provided to Legal Services Penny.O'callaghan@bracknell-forest.gov.uk

Project name	Retender of Casualty Insurance Programme and Claims Handling Service
Department	Corporate Services – Finance
Chief Officer / Head of Service (or delegated officer)	Borough Treasurer
Are members of the public in favour of the project, if so, provide details and refer to supporting evidence	N/A

Instructions for completion

Some cells within the assessment have already been completed and you will need to complete the following cells:

Answer: This response should relate to the question being asked and confirm whether existing controls are already in place e.g. Q1, Yes – Council documentation includes a statement which details how the information will be used and who it will be shared with or No – The Council hasn't informed the individual yet.

Assessment of risk:

In the Assessment of Risk column, score the risk in terms of **Likelihood** and **Impact** using the matrix in **Appendix A** as a guide.

By plotting the numbers on the matrix, you will be scoring them against CMT's tolerance level and you will be able to determine if they are classed as green, amber or red. Enter the appropriate colour in the **Tolerance** cell.

Corrective action/recommendation: You will be able to complete this once you have scored the risk.

Green risks – no further action is required as the risk is at a suitable level

Amber risks – You may need to take further action in an attempt to mitigate the risk down to a green. Fill in the cell if this action is appropriate and consider whether the risk is acceptable at its current level.

Red risks – These are significant risks where attention is required and cannot be tolerated at that current level. You will need to take corrective action to mitigate against the risk.

Priority: This column relates to the priority of the corrective actions and generally should be assessed as:

Red risks – Priority 1 (High)

Amber risks – Priority 2 (Moderate)

Green risks – Priority 3 (Low)

Privacy Impact Assessment

Category 1: Purpose Specification						
Question	Rationale	Answer (Yes/No/N/A)	Risk	Assessment of risk	Corrective action / recommendation	Priority (1,2,3)
1. If personal information is collected will the individual be informed of how it will be used and who, if anyone, it may be shared with?	The purpose of information collection should be stated when the data is collected. Subsequent data use should be limited to stated or compatible purposes. Making your purpose statement available to the public provides greater openness.	Yes At the initial point of the person making the claim, the claim form provides details of who we share information with and what we use their information for	Use of data is not restricted to the original intended purpose or compatible purpose communicated to the individual.	Likelihood score: 1		3
				Impact score: 3		
				Tolerance colour: Green		
2. Is this project needed to deliver services to the public?	The Council can process personal information in order to fulfil its statutory responsibilities. If it is	Yes Informed consent	Consent is not obtained as required.	Likelihood score: 1		3

If not, processing should be with the person's freely given consent.	not necessary in order to provide a statutory service, the processing should be with the person's freely given consent.	is provided by the claimant by the declaration in the claim form		Impact score: 2		
				Tolerance colour: Green		
3. Have the pieces of information the Council needs to collect to fulfil the project's purpose been identified.	Only the amount and type of data needed to achieve a project's purpose should be collected.	Yes The claim form will be the basis of the information collected	Data is collected that is in excess of what is strictly required to deliver the project objectives	Likelihood score: 1		3
				Impact score: 1		
				Tolerance colour: Green		
4. Will there be a review of whether the pieces of information collected are still needed?	Privacy is promoted when the Council reviews whether excessive information is being collected and acts accordingly.	Yes The claim form is reviewed – last review April 2014	Regular reviews are not undertaken to confirm that information still needs to be collected or retained.	Likelihood score: 1		3
				Impact score: 1		
				Tolerance colour: Green		
Category 2: Collection Specification						
Question	Rationale	Answer (Yes/No/N/A)	Risk	Assessment of risk	Corrective action / recommendation	Priority (1,2,3)

5. Will the Council only collect the personal information that is needed for the system's purpose?	The Council should not collect personal information it does not need. Limiting the collection minimises the possible use of inaccurate, incomplete or outdated information. It also reduces the information that can be compromised should a breach occur.	Yes The claim form is the basis for collection of information	Data is collected that is in excess of what is strictly required to meet the purpose of the system.	Likelihood score: 1 Impact score: 1 Tolerance colour: Green		3
6. Will the personal information be obtained by consent? If not, provide details.	Information should be obtained by consent or in a way that is not inappropriately intrusive.	Yes Claimant requests and complete s claim form. Informed consent is obtained through declarati on and signature on claim form	Consent is not obtained for the information collected.	Likelihood score: 1 Impact score: 1 Tolerance colour: Green		3
Category 3: Records Management						
Question	Rationale	Answer (Yes/No/ N/A)	Risk	Assessment of risk	Corrective action / recommendation	Priority (1,2,3)
7. Will there be procedures in place to verify	The Council are required to keep information accurate and when	Yes Claimant	Procedures and controls do not ensure that data	Likelihood score: 1		3

<p>data is accurate, complete, and current?</p>	<p>appropriate, up to date. The Council must make reasonable efforts to minimise the possibility of using inaccurate, incomplete, or outdated information.</p>	<p>expected to notify Insurance Section of any changes in the information they have provided</p>	<p>is accurate, complete and up to date.</p>	<p>Impact score: 3 Tolerance colour: Green</p>		
<p>8. Will information be retained for no longer than necessary? Does the Retention Schedule need to be amended/updated as a consequence of this project?</p>	<p>The Council must not keep personal information for longer than necessary and has a Records Retention Schedule which should be complied with. If amendment is needed to this Schedule, please submit a request form; available at the last page of the Schedule.</p>	<p>Yes</p>	<p>Personal information is not removed when it is no longer required.</p>	<p>Likelihood score: 1 Impact score: 2 Tolerance colour: Green</p>		<p>3</p>
<p>9. Will there be a procedure to provide notice of correction or modification of information to third parties (if any)?</p>	<p>The Council may want to consider establishing logs and audit trails to identify users and third parties that received personal information. This would allow the Council to notify down-the-line users when data are modified from those originally transmitted.</p>	<p>Yes The Insurance Section will inform their claims handling agents of any changes in</p>	<p>There is no clear trail to identify who has been provided with data and end users could potentially be using data that is out of date.</p>	<p>Likelihood score: 1 Impact score: 3 Tolerance colour: Green</p>		<p>3</p>

		informati on provided by the claimant				
Category 4: Use Limitation						
Question	Rationale	Answer (Yes/No/ N/A)	Risk	Assessment of risk	Corrective action / recommendation	Priority (1,2,3)
10. Will the use or disclosure of personal information limited to the purposes it was collected for?	Personal data must be collected for specified, explicit, and legitimate purposes and not used in a way that is incompatible with those purposes.	Yes Informati on only collected for purpose of claim brought against the Council	Personal information is used or disclosed for purposes not intended when it was originally collected.	Likelihood score: 1 Impact score: 2 Tolerance colour: Green		3
11. Will access to personal information be limited to staff/contractors that need the data for their work? If so, describe how.	Employee/contractor access can be limited by policies and procedures or system design. User access should be limited to the information that each employee needs for official duties.	Yes The Council's claims handling agents and insurers have Data Protection policies and this requirement is included	The security of information is not sufficiently robust to ensure it can only be accessed by employees/contractors who need the data for their work.	Likelihood score: 2 Impact score: 2 Tolerance colour: Green		3

		in the terms and conditions of their contract				
Category 5: Security Safeguards						
Question	Rationale	Answer (Yes/No/N/A)	Risk	Assessment of risk	Corrective action / recommendation	Priority (1,2,3)
12. Will there be appropriate technical security measures in place to protect data against unauthorised access or disclosure?	The Council are required to have appropriate technical and organisational measures in place to ensure personal information is protected from unauthorised access, unlawful processing, accidentally loss or destruction of, or damage to personal information.	Yes Data held by Insurance Section only accessed via claims database Figtree which is password protected. Claims Handling Agents have their own database with similar access protectio	System access controls are not sufficiently robust to prevent unauthorised access or disclosure.	Likelihood score: 1 Impact score: 2 Tolerance colour: Green		3

		n					
13. Will there be appropriate physical security in place?	Technical security receives more attention, but physical security is also important.	Yes	Physical access controls are not sufficiently robust to prevent unauthorised access or disclosure.	Likelihood score: 2	Impact score: 2	Tolerance colour: Green	3
14. Will mechanisms be in place to identify: <ul style="list-style-type: none"> • Security breaches? • Disclosure of personal information in error? 	The Council has an Incident Management Reporting Procedure but it should also consider plans to identify security breaches (such as audit trails) or inappropriate disclosures of personal information. Mechanisms should be established to quickly notify affected parties so they can mitigate collateral damage.	Yes	Culture, training and communication of policies and procedures for reporting incidents do not ensure that all significant breaches are reported to the Information Security Officer.	Likelihood score: 1	Impact score: 2	Tolerance colour: Green	3

Conclusion

<p>Comments of Chief Officer/Head of Service</p>	
<p>Approved by Chief Officer/Head of Service</p> <p>Date:</p>	<p>In my view the [potential] privacy intrusion of this project are justified, necessary and proportionate. I agree that the issues raised in this assessment should be addressed</p>

Appendix A

We do not have the resources to manage every risk so we need to establish what risks are most likely to happen and what the impact will be. This allows us to focus our efforts on the highest risks. A Council wide scoring methodology of impact and likelihood has been developed to help establish if risks are above the tolerance level determined by CMT. This is set out in the simple risk matrix below:

LIKELIHOOD	5					
	4					
	3					
	2					
	1					
		1	2	3	4	5
	IMPACT					

LIKELIHOOD:

5 Very High

4 High

3 Significant

2 Low

1 Almost Imp

IMPACT:

5 Catastrophic

4 Critical

3 Major

2 Marginal

1 Negligible

The scoring of risks is a judgement based assessment but the following can be used as a guide for assigning scores to risks.

CRITERIA FOR ASSESSING LIKELIHOOD

PROBABLILTY	SCORE	DEFINITION
Almost impossible	1	Rare (0-5%).The risk will materialise only in exceptional circumstances.
Low	2	Unlikely (5-25%). This risk will probably not materialise.
Significant	3	Possible (25-75%). This risk might materialise at some time
High	4	Likely (75-95%). This risk will probably materialise at least once.
Very High	5	Almost certain (>95%). This risk will materialise in most circumstances.

Note: the timeframe over which the risk should be assessed should usually be the one-year time frame of the Service Plan or the life of a particular Project/Programme or Partnership – dependent upon the level of risks being considered.

CRITERIA FOR ASSESSING IMPACT

	Negligible	Minor	Major	Critical	Catastrophic
Score	1	2	3	4	5
Disruption to established routines/operational delivery	No interruption to service. Minor industrial disruption.	Some disruption manageable by altered operational routine.	Disruption to a number of operational areas within a location and possible flow to other locations.	All operational areas of a location compromised. Other locations may be affected.	Total system dysfunction. Total shutdown of operations
Damage to reputation	Minor adverse publicity in local media.	Significant adverse publicity in local media.	Significant adverse publicity in national media.	Significant adverse publicity in national media. Senior management and/or elected Member dissatisfaction.	Senior management and/or elected Member resignation/removal.
Security	Non notifiable or reportable incident.	Localised incident. No effect on operations.	Localised incident. Significant effect on operations.	Significant incident involving multiple locations.	Extreme incident seriously affecting continuity of operations.
Financial (Organisation as a whole or any single unit)	<1% of monthly budget	>2% of monthly budget	<5% of monthly budget	<10% of monthly budget	<15% of monthly budget

	Negligible	Minor	Major	Critical	Catastrophic
Score	1	2	3	4	5
General environmental and social impacts	No lasting detrimental effect on the environment i.e. noise, fumes, odour, dust emissions, etc. of short term duration	Short term detrimental effect on the environment or social impact i.e. significant discharge of pollutants in local neighbourhood.	Serious local discharge of pollutants or source of community annoyance within general neighbourhood that will require remedial attention.	Long term environmental or social impact e.g. chronic and significant discharge of pollutants.	Extensive detrimental long term impacts on the environment and community e.g. catastrophic and/or extensive discharge of persistent hazardous pollutants.
Corporate management	Localised staff and management dissatisfaction.	Broader staff and management dissatisfaction.	Senior management and /or elected Member dissatisfaction. Likelihood of legal action.	Senior management and/or elected Member dissatisfaction. Legal action.	Senior management and/or elected Member resignation/removal.
Operational management	Staff and line management dissatisfaction with part of a local service area.	Dissatisfaction disrupts service.	Significant disruption to services.		Resignation/removal of local management.
Workplace health and safety	Incident which does not result in lost time.	Injury not resulting in lost time.	Injury resulting in lost time. Compensatable injury.	Serious injury /stress resulting in hospitalisation.	Fatality (not natural causes)