

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 its 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.

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 1 October 2017
DATE AGREED	
NEXT REVIEW DATE	
AGREED BY	
COVERAGE	
AUTHOR(S)	Jon Richardson Joint Commissioning Officer Alison Cronin, Contracts and Procurement Manager Neil Haddock, Chief Officer: Commissioning and Resources

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: October 2017	Directorate: Adult Social Care, Health & Housing	Section: Adults & Joint Commissioning
1. Project to be assessed	Signing up to 4 Nursing Block Contracts for people over 65	
2. Officer responsible for the screening	Jon Richardson, Joint Commissioning Officer	
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 type="checkbox"/> New <input checked="" 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 type="checkbox"/> Collecting new Personal Information <input checked="" 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	Entering into Nursing Block Contracts for people over 65 will <ul style="list-style-type: none"> • provide greater choice to service users wishing to utilise a local nursing placement. • provide a much needed increase in affordable local bed capacity. • improve competition within the local Nursing care market. • respond to changing needs and demands. 	

8. On the basis of sections 5 and 6 above is a full impact assessment required?	Y <input checked="" type="checkbox"/>	N	<p>Please explain your decision. If you are not proceeding to a full Privacy Impact Assessment make sure you have the evidence to justify this decision should you be challenged.</p> <p>Whilst this is not a new service and we will continue to need to make nursing placements; a full Privacy Impact Assessment is required due to boxes ticked in section 5 & 6.</p>
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
N/A			
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

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

Yes, undertaken.

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

Project name	Nursing Block Contract
Department	ASCH&H
Chief Officer / Head of Service (or delegated officer)	Chief Officer: Adults and Joint Commissioning
Are members of the public in favour of the project, if so, provide details and refer to supporting evidence	Yes This is not a new service. Where people require a nursing placement, they and their family are entitled to have a choice of local provision. This project is intended to increase affordable local options.

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.	Y	Use of data is not restricted to the original intended purpose or compatible purpose communicated to the individual.	Likelihood score:2	Nursing Providers will not have access to any sensitive information from the Council without the explicit consent of the individual within a signed agreement from the person using the nursing service and/or their representative (where there are issues of capacity). Explicit consent can only be obtained by the Nursing Provider through providing a comprehensive explanation of the intended purpose, so that the individual can make an informed decision whether or not to give their consent. The Council shall ensure that the Nursing Provider has an Information Sharing Protocol in place with other organisations for secure information sharing.	3
				Impact score: 2		
				Tolerance colour:GREEN		

					Nursing Providers are registered under Care Quality Commission and are required to abide by the regulations set under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014. This includes the collection and retention of personal information.	
2. Is this project needed to deliver services to the public? If not, processing should be with the person's freely given consent.	The Council can process personal information in order to fulfil its statutory responsibilities. If it is not necessary in order to provide a statutory service, the processing should be with the person's freely given consent.	Y	Consent is not obtained as required.	Likelihood score: 2	The Council has the power to share personal data in accordance with Schedule 2, paragraph 5 of the Data Protection Act 1998. If personal information is to be shared then the Council will need to receive from the Nursing Provider a signed form from the person using the nursing service, providing explicit consent to share personal information. Explicit consent can only be obtained by the Nursing Provider through providing a comprehensive explanation of the intended purpose, so that the individual can make an informed decision whether or not to give their consent. The Council will ensure that	2
				Impact score:3		
				Tolerance colour:AMBER		

					<p>the Provider is able to offer evidence of appropriate policies and processes are in place.</p> <p>The Council shall ensure that the Nursing Provider has an Information Sharing Protocol in place with other organisations for secure information sharing.</p>	
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.	Y	Data is collected that is in excess of what is strictly required to deliver the project. objectives	<p>Likelihood score:2</p> <p>Impact score:2</p> <p>Tolerance colour:GREEN</p>	<p>The Council will enter into a data sharing agreement with Nursing Providers to ensure that no data is collected excessively, is collected only on a need to know basis and any data collected will be subject to a review. The Council will require Nursing Providers to demonstrate and provide assurances that personal information and data is gathered for the specific purpose to help with the care and/or support of an individual.</p> <p>The Council shall ensure that the Nursing Provider has a policy in place to comply with this requirement.</p>	3
4. Will there be a review of whether	Privacy is promoted when the Council	Y	Regular reviews are not	Likelihood score:2	When any information concerning a person using	3

the pieces of information collected are still needed?	reviews whether excessive information is being collected and acts accordingly.		undertaken to confirm that information still needs to be collected or retained.	Impact score:2	the nursing service is requested (with their authority) the Practioner will need to ensure it is on a need to know basis for a specific issue or identified as required. The Council will enter into a data sharing agreement with Nursing Providers to ensure that no data is collected excessively, is collected only on a need to know basis and any data collected will be subject to a review. The Council shall ensure that the Provider has a policy in place to comply with this requirement. Checks will be undertaken as part of the contract monitoring process.	
				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	Y	Data is collected that is in excess of what is strictly required to meet the purpose of the system.	Likelihood score:2	Where personal information is to be shared then the Council will need to receive from the Nursing Provider a signed form from the person receiving the nursing service providing authority	3
				Impact score:2		

	or outdated information. It also reduces the information that can be compromised should a breach occur.			Tolerance colour:GREEN	to share personal information. The terms of the information sharing will also be set forth within the form. The Council shall ensure that the Nursing Provider has an Information Sharing Protocol in place with other organisations for secure information sharing. Where personal information is to be shared then the Nursing Provider will need to receive from the organisation a signed form from the person providing authority to share personal information. The terms of the information sharing will also be set forth within the form. The Council will be consulted and will review the Information Sharing Protocol between Nursing Provider and the other organisations it will be sharing data with, and to be a signatory to the protocol.	
6. Will the personal information be obtained by consent? If not,	Information should be obtained by consent or in a way that is not inappropriately intrusive.	Y	Consent is not obtained for the information collected.	Likelihood score:2 Impact score:2	The Nursing Provider, if asking for information regarding a person using nursing services in order to help with the care or	3

provide details.				Tolerance colour:GREEN	support, will need to provide the council with a signed consent form from the person. This requirement will be included in the data sharing agreement between the Council and Nursing Provider.	
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 data is accurate, complete and current?	The Council are required to keep information accurate and when appropriate, up to date. The Council must make reasonable efforts to minimise the possibility of using inaccurate, incomplete, or outdated information.	Y	Procedures and controls do not ensure that data is accurate, complete and up to date.	Likelihood score:2	An assessment will be undertaken by the Practitioner at the review stage as to whether the information is relevant, and up to date. This requirement will be included in the data sharing agreement between the Council and Nursing Provider.	3
				Impact score:2		
				Tolerance colour:GREEN		
8. Will information be retained for no longer than necessary? Does the Retention	The Council must not keep personal information for longer than necessary and has a Records Retention	Y	Personal information is not removed when it is no longer required.	Likelihood score:2	The Contract with the Nursing Provider will include a Records Retention Schedule to ensure that personal	3

Schedule need to be amended/ updated as a consequence of this project?	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.			Impact score:2	information is not kept longer than necessary.	
				Tolerance colour:GREEN	The Council will require Nursing Providers to demonstrate assurances of how information is collected, stored securely and retained.	
					Checks will be undertaken as part of the contract monitoring process	
9. Will there be a procedure to provide notice of correction or modification of information to third parties (if any)?	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.	Y	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.	Likelihood score:2	A log of all those people, using nursing services who have requested that their care information can be shared with the contracted Nursing Provider and voluntary sector organisations will be kept by the Council.	3
				Impact score:2	The Council shall ensure that the Nursing Provider has a policy in place to comply with this requirement.	
				Tolerance colour:GREEN	This requirement will be included in the data sharing agreement between the Council and Nursing Provider.	
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.	Y	Personal information is used or disclosed for purposes not intended when it was originally collected.	Likelihood score:2	<p>The Council will require the Nursing Providers to demonstrate assurances that personal information is only used and disclosed for the specific purpose to help with the care and/or support of an individual.</p> <p>The Council shall ensure that the Nursing Provider has a policy in place to comply with this requirement.</p> <p>This requirement should be included in the data sharing agreement between the Council and Nursing Provider.</p> <p>A log of this information will be kept and audited annually by the Council.</p>	3
				Impact score:2		
				Tolerance colour:GREEN		
11. Will access to personal information be limited to staff/contractors that need the data for their work?	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	Y	The security of information is not sufficiently robust to ensure it can only be accessed by employees/contractors	Likelihood score: 2	The information will only be shared once the Council has received a signed form from the person using nursing services giving consent for information to be shared from the	3
				Impact score:2		

<p>If so, describe how.</p> <p>The information will only be shared once the council has received a signed form from the resident giving consent for information to be shared) from the provider.</p>	for official duties.		ctors who need the data for their work.	Tolerance colour:GREEN	<p>Provider. This requirement will be included in the Information sharing Protocol.</p> <p>The Council shall ensure that the Nursing Provider has an Information Sharing Protocol in place with other organisations for secure information sharing. The Council will be consulted and will review the Information Sharing Protocol between the Nursing Provider and the other organisations it will be sharing data with, and to be a signatory to the protocol.</p>	
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.	Y	System access controls are not sufficiently robust to prevent unauthorised access or disclosure.	Likelihood score: 2	<p>The Nursing Provider will be required to sign the Council's ICT third Party standards document.</p> <p>The Nursing Provider will ensure where appropriate, an IT Information Sharing Protocol is in place with organisations for secure information sharing.</p>	3
				Impact score:2		
				Tolerance colour GREEN		
13. Will there be	Technical security	Y	Physical access	Likelihood	Any physical information	3

appropriate physical security in place?	receives more attention, but physical security is also important.		controls are not sufficiently robust to prevent unauthorised access or disclosure.	score:2	concerning individuals should be kept in locked filing cabinets. The Nursing Provider will take appropriate steps to ensure personal data remains secure outside of the premises when visiting People. This requirement will be stated within the data sharing agreement between the Council and Nursing Provider. The Council shall ensure that the Nursing Provider has a policy in place to comply with this requirement. Nursing Providers are registered under Care Quality Commission and are required to abide by the regulations set under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014. This includes the collection and retention of personal information.	
				Impact score:2		
				Tolerance colour:GREEN		
14. Will mechanisms be in place to identify: • Security breaches? • Disclosure of personal	The Council has an Incident Management Reporting Procedure but it must also consider plans to identify security breaches (such as audit trails) or inappropriate	Y	Culture, training and communication of policies and procedures for reporting incidents do not	Likelihood score:2	As part of the Contract, the Council will require the Nursing Provider to adhere to the Council's "Incident Management Reporting Procedure" and ensure existing physical security	3
				Impact score:2		

information in error?	disclosures of personal information. Mechanisms should be established to quickly notify affected parties so they can mitigate collateral damage.		ensure that all significant breaches are reported to the Information Security Officer.	Tolerance colour:GREEN	arrangements will be adhered to. The Nursing Provider will stipulate and ensure where appropriate, an Information Sharing Protocol is in place with organisations for secure information sharing.	
-----------------------	---	--	--	------------------------	--	--

Conclusion

Comments of Chief Officer/Head of Service	No comments
Approved by Chief Officer/Head of Service Date:	 3/10/2017 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

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						<u>LIKELIHOOD:</u>
	4						5 Very High
	3						4 High
	2						3 Significant
	1						2 Low
		1	2	3	4	5	1 Almost Imp
							<u>IMPACT:</u>
							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)