Appendix 2

PRIVACY IMPACT ASSESSMENT

Electronic Care Brokerage

Document Control

Organisation	Leeds City Council
Title	Privacy Impact Assessment
Author	Yvonne Roberts / Helen Gibson
Filename	
Owner	
Subject	Data Protection
Protective Marking	Not Protectively Marked
Review date	

Version Control

Version	Status	Revision Date	Summary of Changes	Author
0.1	Draft	09 July 2015	First Draft	Georgia Young
0.2	Draft	13 July 2015	Amendments following further information gathering	Helen Gibson
0.3	Draft	14 July 2015	Further updates including comments from Yvonne Roberts	Helen Gibson
0.4	Draft	15 July 2015	Further updates including from discussion with ICO Louise Whitworth, and comments from Jason Lane	Helen Gibson
1.0	Final	15 July 2015	Version for ICO approval. Then to continue to be built on, and approved by ASC Commissioning.	Helen Gibson
1.01		20 July 2015	Updates included following comments from Michelle Atkinson and Georgia Young	Helen Gibson
1.02		3 August 2015	Updates following further clarifications with ICT, preferred supplier, Michelle Atkinson and Jason Lane.	Helen Gibson
1.03		3 August 2015	Updates from Martyn Tinsley – ICT Services	Martyn Tinsley
1.04		4 August 2015	Updates to Appendix A.	Helen Gibson
1.05		21 August 2015	Updates, including from discussion with Louise Whitworth and in relation to CIS integration.	Helen Gibson
1.06		7 October 2015	Updates including related to LCC staff data content, data retention, and supplier penetration testing	Helen Gibson
2.0		14 October 2015	Updates following comments from Martyn Tinsley (ICT), Lisa Powell (ASC IM&T) and Louise Whitworth	Helen Gibson

Introduction

Privacy impact assessments (PIAs) are a tool to identify and reduce privacy risks. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help design more efficient and effective processes for handling personal data.

The document must be completed for any new / or change in service where personal or personal sensitive information is used. It must be completed as soon as the new service / or change is identified by the Project Manager / System Manager or Information Asset Owner.

This process is a mandated requirement by the Information Commissioners Office and the Information Governance Toolkit to ensure that information risks and privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal and personal sensitive information.

There are 2 types of Privacy Impact Assessments; a small scale and a full scale. This template is based on the Small Scale PIA. Following completion of this template, it may be necessary to conduct a Full Scale PIA. Further details are available on the Information Commissioners website. www.ico.gov.uk

Please complete all questions with as much detail as possible and return the completed form to your Directorate Information Compliance Officer. Details can be found on Insite. http://insite.leeds.gov.uk/toolkits/Pages/Managing-information.aspx

Brief guidance regarding the Data Protection Principles and a Glossary of Useful Terms can be found at the end of this document. If you require any further assistance in the completion of the document, please contact you Directorate Information Compliance Officer.

Section A: New/Change of System/Project General Details

Name: (of the project or change to be delivered)	Home Care Redesign and Commissioning Project – Electronic Care Brokerage (Phase 1 ASC generic home care commissioning)
Background: (why is the new system / change required?)	Adult Social Care embarked on an ambitious modernisation programme in order to improve its information management, information sharing and information security. As part of this, work was taken forward to purchase a system for publishing new home care packages to a secure website, accessible to predetermined groups of homecare providers, thereby supporting the work of officers engaged in brokering homecare. A procurement process began in summer 2013 and a preferred supplier was identified in early 2014, with permission granted to enter into negotiations. In autumn 2014 this activity was brought into the scope of the Home Care Redesign and Commissioning project, established to review, improve, implement and evaluate the service delivery model, procurement and contracting approach for independent sector home care provision in Leeds. In 2015 a review of whether the statement of requirements was still fit for purpose was undertaken given wider changes, with subsequent clarification and negotiation with a view to awarding the contract in Autumn 2015.

Benefits: (explain what the project aims to achieve, what benefits to the organisation, to individuals and to other parties)	Benefits of the overarching Home Care project include: • ASC will meet its statutory obligations. • Implementation of national and local policies and guidance relating to home care and personalisation will be facilitated. The Electronic Care Brokerage (ECB) system will make significant improvements and efficiencies to the processes used by officers in the Care Communications Centre (CCC) to broker homecare, replacing the current inefficient paper, fax and telephone based manual systems that require considerable administrative resource. The new web-based system should • securely direct all service requests to the appropriate contractor(s) using the service user's postcode. The greater data security offered by a secure website, accessible only to pre-determined groups of providers under contract should facilitate the provision of more detailed care package requirements, and secure transmission of enquiries • increase the speed of distribution of care packages, and more rapid confirmation of acceptance of a care package, producing a positive outcome for home care service users • have the facility to automatically generate comprehensive management reports regarding the take up and delivery of home care packages, for better data management • make available more focussed information enabling providers to make a better more personalised offer to deliver, and enable service users to be given more information about a provider or providers • enable a better match between the outcomes selected by the service user and the offered care package to support the delivery of the outcomes.
Constraints:	Time – must be in place in readiness for the new home care contracts, which commence on 1 June 2016. Cost – there is a designated budget for the ECB system and related work on a monitoring system; solutions must be delivered within the budget. Quality – The system must be fit for purpose as defined by ASC Commissioning, these are set out in the tender specification for the ECB system, in addition standards will be identified in documents to be developed e.g. Quality Strategy and subsequent testing strategies and requirements for sign off of products. All LCC quality standards will be adhered to when developing and implementing the outputs / products e.g. relating to Data Protection and Information Governance, and new project management methodology
Relationships / Partnerships: (e.g. with NHS, or private organisation)	• Contracted home care providers. • ECB system supplier. There are is a possibility that access to the system will be extended to NHS health colleagues at a later date, alternatively information may be made available to them via LCC teams that have access. Health staff with a potential interest include hospital Discharge Co-ordinators, and Continuing Care. This will be kept under review in light of the Integration Programme.

	Other relationships are within Leeds City Council e.g. Access and Care Teams in ASC.	
Project Manager:	Name:	Georgia Young
	Title:	Project Leader
	Service:	Programme Management Office
	Telephone:	07891 276012
	Email:	georgia.young@leeds.gov.uk
Information Asset Owner All information assets must have an information asset owner (IAO). IAO's are usually Heads of Service or Chief Officers. For further information regarding IAO's please contact your directorate InCo, details of which can be found in the Managing Information Toolkit on InSite.	Name:	Mick Ward
	Title:	Head of ASC Commissioning
	Service:	Adult Social Care Strategic Commissioning
	Telephone:	0113 37 83912
	Email:	Mick.Ward@leeds.gov.uk
System Administrator (if applicable)	Name:	To be determined. Responsibility may sit within ASC IM&T.
	Title:	
	Service:	
	Telephone:	
	Email:	

Section B: Privacy Impact Assessment

(please complete all questions as fully as possible)

Question	**Response**	**References**
1. Will the system / project / process (will now be referred to thereafter as 'asset') contain Personal or Sensitive Personal data/information? (If answered 'No' you do not need to complete any further information as PIA is not required)	☐No ☒Citizen / Service User ☐Employee ☐Other (please specify) No personal information of external provider staff is expected to be input to the ECB system. Personal data in the form of the name and work phone number of the ASC care manager or social worker for a service user may be used in the ECB system, this is already made available to providers as part of information in Individual Service Agreements (ISAs). The final content of service request data to be input to the ECB system is yet to be finalised, and a business exercise is planned to review the personal data involved in ECB (relates also to question 7).	See Glossary for definitions See Section C related risk and solution

2. Please state the purpose for the collection of the data / information: (for example, service provision, research, audit, employee administration)	To broker home care provision and ensure services offered meet the needs of service users and are contract compliant.	
3. Does the asset involve privacy invasive technologies?	☒Yes (if yes, please give details) Brokerage system may be used to produce maps showing locations of service users, and which providers are delivering their care. ☐No	See Glossary for definitions
4. Please tick the data items / information that will be held as part of this asset.		
Personal	☒Name ☒Address ☒Postcode ☒Date of Birth ☒Next of Kin (please note, may involve other information such as Carer details on ASC assessment and support plan documents. Action to clarify what is held on CIS and will be shared) ☐National Insurance Number ☒NHS Number (to be confirmed) ☒Gender ☒GP / Consultant	See Glossary for definitions
Sensitive	☒Sexual Orientation ☒Religion ☒Occupation ☒Ethnic Origin ☒Medical History ☒Care plan ☒Appointment dates	See Glossary for definitions
Other (please specify)	Information relating to safeguarding of service users, household members and staff including domestic violence information, household members who may pose risk to staff. Information relating to criminal offences, e.g. service user or household member (only where a relevant risk to the delivery of care e.g. speeding offences are irrelevant but sexual assault may be). Information regarding the domestic environment that the service will be delivered in e.g. access arrangements. Information regarding service user medicine	

	support, and planned hospital admission or discharge dates. The amount of care and outcomes chosen and choices regarding care made.	
5. Will the asset collect new personal data items which have not been collected before?	☐Yes ☒No All of the information about service users should have been collected by Access and Care staff and be recorded on CIS prior to being entered into the ECB.	
6. The data of approximately how many individuals will be affected by this asset?	Data will be recorded as and when homecare provision needs to be brokered. Volumes to be confirmed: • Service users – 3,500 to 4,000 plus • Next of kin/emergency contacts, and • Household members, e.g. those that pose a risk. • May include name and contact details of the ASC care manager / social worker involved	
7. What checks have been made regarding the adequacy, relevance and necessity for the collection of personal and / or personal sensitive data for this asset? See Section E for references to Data Protection Principles.	See Appendix A, where information is provided with reference to the Data Protection Principles (previous section E). Includes some areas for further action that are also logged in section C.	If no checks have been made please record this as a risk in section C See Section C related risk and solution
8. Who provides the information for the asset?	☐Citizen / service user ☒Employee – Access and Care from CIS ☐Other (please specify e.g. integration with another system)	
9. Are you relying on individuals to provide consent for the processing of this personal and / or personal sensitive data	☒Yes ☐No	
10. If yes, how will that consent be obtained and recorded? (please state)	During the assessment/review process undertaken by Access and Care staff and service providers (in terms of reviews). Longer term, if NHS health staff have access to the system they will need to obtain consent. Consent will be recorded on CIS – see Section C.	See Section C related risk and solution
11. Have the individuals been informed of this processing?	☒Yes (explicit) ☐Yes (implicit i.e. through fair processing notice, website, leaflet etc) ☐No Fair Privacy Notices and consent forms have been amended. To review whether additional or revised guidance needs to be provided to assessors and care managers regarding how the service user and carer data will be used and what to tell them. See also Appendix A re. data principle 1.	If no please record as a risk in section C See Section C related risk and solution

12. How will the information be kept up to date and checked for accuracy and completeness?	Users of the system will have guidance on what they need to complete, and CCC will check all service requests before they are published to providers. We will review how, and how well, the system and process encourages accuracy of information completion e.g. extent of field validation, including during testing, and the guidance for system users. Once the brokerage process has been completed, information in the system will not be changed or amended unless there is a new brokerage request. Any changes to service user information will be made via CIS. CIS is a record system where information needs to be updated. The ECB asset is a brokerage system so offers only a snapshot of what was brokered at that time.	If there are no documented procedures to evidence this answer, please record as a risk in section c See Section C related risk and solution
13. Who will access the information? (Services, roles, organisations?)	Who is expected to input or access information for day to day use: • LCC Access and Care e.g. social workers in ASC • LCC CCC – all staff, management and care communication officers (7 people) • LCC Business support managers – in Access and Care Teams • Service providers – varying roles depending on organisational structure of each service. Will only see data related to work they are offered to consider, and remain able to see data for work they then take on. • Brokerage system supplier • LCC ASC Commissioning staff – some managers and officers • LCC ASC Contracts Team – some managers and officers • LCC ASC Performance Quality Assurance team – possibly via CCC rather than direct access but work ongoing to clarify the approach. • LCC ASC IM&T e.g. related to system administration NHS staff– may have access in the future but not currently in scope. Who may be able to access information given their role in managing or hosting systems: • Staff working for the third party server host (on behalf of the system supplier) • LCC Staff in ICT – data security, service desk (where support is provided by LCC rather than system supplier)	See Section C related risk and solution
14. Is there an Access Control Policy in place?	☐Yes	If no please record as a risk in section C.

	☒No Not currently but there will be. Access Control Policy to be created including, clarification of different access levels for different groups of users that restricts what they can see or do. The ECB system has an access schema that will need then to be populated. After a pre-determined period of inactivity on the system a user will be timed out and will need to log in again. The timeout of the system is expected to be about 10-15 minutes, and this will be reviewed in the testing phase, taking into account usability and security. See also information noted under question 24 related to system security.	See Glossary for definition See Section C related risk and solution See Section C related risk and solution
15. Is there a usable audit trail in place for the asset? E.g. to identify who has accessed a record	☒Yes ☐No This was one of the requirements when the system was procured therefore will be in place when system goes live.	If no please record as a risk in section C. See Glossary for definition
16. What are the retention periods for this asset?	ASC have advised that the retention period for all records is 6 years from cessation or termination of the contract, in line with legal contract retention periods. This refers to the date of the termination or completion of each brokered care package within the new system. However, ASC's intention is that the system is for brokerage purposes only, and that the contracts for each care package offer and acceptance that are generated by the system will themselves be stored separately, this is expected to be in the CIS system. Processes and details are to be confirmed. Where additional data is on the system that may be subject to other retention schedules it will be a duplicate record e.g. uploaded by Access and Care from EDRMS, or present on CIS. In addition if a provider uploads content that needs to be retained in such a way, e.g. from a review of needs, Access and Care will make sure it is also held on their case management system. The preferred supplier's ECB system will archive records after 7 years inactivity, and information on asset destruction is noted below (question 17). Current contracting plans with the supplier are for up to 3 years. Following consideration by Information Governance the costs associated with developing the system to	If there are no documented retention periods please record as a risk in section C

	deal with the earlier archiving and/or destruction of records and addition of disposal rules do not appear to be worthwhile, as nothing will need to be destroyed within the period we will be using the system. Should a decision be taken to keep the system longer i.e. closer to 7 years, we will need to review this. In addition, for future commissioning of a brokerage system the essential requirements for disposal and destruction of information will need to be included in the specification.	
17. How will the asset be destroyed when it is no longer required?	At the end of contract with the system supplier, or within 2 months of notice being given by LCC, the supplier will : • provide data cuts and partial and full database dumps for transition to any replacement system. The full field set of fields held by the system is made available and is transmitted in a standardised format to give the greatest compatibility with third party systems and tools; • attend a final handover meeting to review Leeds data held on systems; and • ensure that the services provided are appropriately de-commissioned. All data held on their systems belonging to Leeds will be deleted and destroyed and they will provide a written certificate confirming the date, time, place and means by which all data was deleted and destroyed.	
18. Will the asset or part of the asset be shared with other organisations?	☒Yes ☐No Home care providers, the brokerage system supplier and their third party server host organisation.	If yes please record as a risk in section C
19. If yes, are there appropriate information sharing agreements in place	☐Yes ☒No Provision was made in the original procurement terms and conditions in relation to the ECB system supplier, however following updates to Council policy these arrangements are being reviewed for contract award. Following review by ASC Information Governance the provisions within the Terms and Conditions to be used are considered completely adequate, no changes are needed. Home care provider information governance agreements are being put in place as part of the	If no please record as a risk in section C See Section C related risk and solution

	separate home care provider procurement activity.	
20. Please list all organisations involved	- LCC - Home care providers to be confirmed when home care contracts have been awarded (Dec 2015). Potentially a minimum of 6, no maximum – currently 30+ on the framework agreement. Will be included in contract terms. - Existing home care service providers where we ask them to participate in any pilot or testing of the system before it goes live (any pilot or testing does not currently plan to include personal information from real service users) - Brokerage system supplier - Third party server host organisation NHS involvement through Health / Discharge Co-ordinators is not currently within scope.	
21. Does the asset involve new linkage / matching of personal data with data in other collections, or is there significant changes in data linkages / matching?	☒Yes ☐No Integration with CIS is planned for a future phase (post go-live). However, there is a risk that this will not be possible, resulting in ongoing double entry of brokerage information. The requirements and feasibility for this integration work is to be undertaken at a later date, and implementation will be reliant on the capabilities of the preferred supplier's system as well as value for money. Some documents will be uploaded (copied) to the ECB from the EDRMS (Sharepoint). The master record will remain the version in the EDRMs, not the ECB system. Providers may also upload documents to ECB. The ECB system will electronically link service user information with their home care requirements and a home care provider. Where information on ECB is not already held in CIS it may need to be exported to the LCC ASC data warehouse. For information: Another planned system related to monitoring, the Home care analysis and information tool (HCAIT), is planned to link certain information held on ECB about home care commissioned with information sent by providers from electronic care monitoring data to compare what was requested versus provided to service	If yes please record as a risk in section C. See Glossary for definition, As advised by ICO Louise Whitworth, no risk to be recorded as matching is of LCC owned data only.

	users e.g. for invoicing purposes. A separate PIA will be considered for this.	
22. Where will the asset be stored / accessed?	☐On paper ☐On a network folder / drive ☒Website ☒Dedicated system ☒Other (please state below) The asset involves an app server, web server, and database server, with content populated by LCC and by the external home care providers. The servers are provided by the external brokerage system supplier, with the farm of servers hosted in a third party data centre (Rackspace) which is based in Slough, UK.	
23. Will any information be sent off site? (i.e. a building or network not under the direct control of LCC)	☒Yes ☐No All content will be stored off site at the Rackspace data centre in Slough, UK– see also question 24 response	If yes please record as a risk in section C
24. If yes, please state by which method the information will be transported	☐Fax ☐Standard email ☐Secure email (e.g. GCSx) ☒Website ☐Via courier ☐By hand ☐Via external post ☐Via telephone ☒Other (please state below) *Appendix A – Principle 7* provides full details of the proposed security of the system. The information below provides a brief summary of the key points. Home care provider organisations will view and respond to home care packages using the secure ECB portal, with CCC controlling which providers are able to view and access each package. The solution is fully hosted in the UK, with the third party server host adhering to ISO17799 (Information technology - Security techniques - Code of practice for information security management), which is regularly reviewed as part of their SAS70 (Statement on Auditing Standards for	See Section C related risk and solution

	service organisations) Type II audit process. In addition the preferred supplier is fully accredited to ISO 27001. Data in transit is secured with HTTPS and is encrypted using the Transport Layer Security (TLS) protocol (which is a more secure successor to Secure Sockets Layer SSL). This means that the network traffic between the user's browser and the server is encrypted. The provider of the ECB system (Oxford Computer Consultants) currently supports older versions of the TLS encryption protocol (versions 1.0 and 1.1) to ensure compatibility with older web browsers. Use of these older versions is an acceptable risk in the short term. However, from June 2016, Oxford Computer Consultants will cease support for these older versions of TLS (v1.0 and v1.1) in order to maintain a high level of security on the system. The supplier will require a domain name and certificate to be provided by council, and can support any strength and version that LCC require. LCC has required a 2 factor authentication approach using SMS for delivery of tokens, which the supplier will deliver. There are ongoing revenue costs to LCC for this use. The strength of user passwords is configurable by LCC (e.g. length and inclusion of both alpha and numeric characters). It will be possible to change passwords (e.g. if forgotten etc.) but it will not be possible to force their renewal (e.g. every 90 days as with the internal LCC password policy). Other authorities using the same system supplier have undertaken penetration testing of the system in the summer and autumn 2015, including testing against the OWASP Top 10, and information has been shared with LCC. The supplier has also undertaking its own penetration testing in August 2015, and the results and resulting actions were provided to LCC. From the most recent test we have seen it appears that any key issues arising have been resolved by the supplier or appropriate plans are in place e.g. to stop supporting TLS v1.0 and v1.1) encryption standards by end June 2016. LCC plan to test the security of the system prior to go-live and also undertake periodic penetration testing when the system is live.	

	The data and back-ups of the data are held at different UK locations. The data server is also in the UK. See *Appendix A – Principle 7* for full details of: • The preferred supplier accreditation • User Account Management • Password Policy • Password Strength • Two factor Authentication • Security of data in transit • Security Penetration Testing • Secure Integration to CIS	
25. Are you transferring any personal and / or personal sensitive information to a country outside the European Economic Area (EEA) If yes, where?	☐Yes ☒No	If yes please record as a risk in section C
26. Is there a contingency plan / back up policy in place to manage the effect of an unforeseen event?	☒Yes ☐No As standard Rackspace do not offer failover should their entire data centre be rendered inoperable, and so business continuity plans will need to be used in the event of major unforeseen events, until the problems are resolved by the ECB supplier or third party data centre. Rackspace do however have multiple redundancy for their comms to reduce the likelihood of connectivity issues. Full backups are taken and stored off-site from the primary datacentre, allowing recovery from more significant disasters or corruption. ASC to review their business continuity plan(s) in order to define the process that will be taken by CCC and external providers in the event of an unforeseen event that means the ECB system cannot be used/accessed for a period of time.	If no please record as a risk in section C See Section C related risk and solution See Section C related risk and solution

Section C: Identify the Information, Privacy and related risks

Identify the key risks. All risks identified from the questionnaire in section B should be included, plus any others of relevance. Describe the actions you could take to reduce the risks and any future steps which would be necessary (e.g. the production of new procedures or future security elements for systems).

Risk	**Solution**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution justified, compliant and proportionate response to the aims of the project?
Personal data is not obtained for any purposes that are not specified and lawful	(see PIA question 1 and 7 and Appendix A DP2) Review needed of project plan to make sure it covers all of the specified and lawful purposes for processing personal data.	Reduced	
Personal data is not processed where it is inadequate, irrelevant or excessive in relation to purpose	(see PIA question 1 and 7 and Appendix A DP3) Business exercise needed to review the personal data involved in ECB, with output to be attached to this PIA.	Reduced	
Individuals (service users) are not informed of this processing of their data	(see PIA question 11, and Appendix A: DP1) Fair Privacy Notices and consent forms and scripts have been amended. To review whether additional or revised guidance needs to be provided to assessors and care managers regarding how the service user and carer data will be used and what to tell them – part of Workforce Development activity.	Reduced	
Data is still processed for those individuals that do not provide consent	(see PIA question 10) Information on **service user** consent will be captured on CIS. Need to clarify business processes, and have procedures in place, to make sure that home care packages are not brokered where consent is not given. Both in the interim arrangements where CIS does not integrate with ECB, and for when/if it does.	Reduced	
New systems do not provide protection against identified security risks.	(see PIA questions 24 and 7 and Appendix A DP7 linked to external hosting and security of web-based systems.) Clarifications on security certification and controls, and password strength have been received from the supplier, following queries by ICT colleagues on security elements. And LCC needs in relation to two-factor tokens for user identification have been met. References from other authorities that are live customers of the preferred system supplier, using a related system, have been very positive.	Reduced	Confirmed

	Penetration test results undertaken by another authority have been shared, with any issues acted on swiftly by the supplier. The results from supplier’s own testing in August using SureCloud have been received and issues acted on by the supplier. From the most recent test form another authority that we have seen it appears that any key issues arising have been resolved by the supplier or appropriate plans are in place e.g. to stop supporting browsers with lower (TLSv1.0) encryption standards by end June 2016. LCC plan to take forward their own periodic penetration tests post go-live. Following advice from our security experts, no additional testing is needed prior to contracting.		
Information is not kept up to date and checked for accuracy and completeness	(see PIA question 12 and Appendix A DPA4) Planned procedures to be documented in relation to **managing changes and amendments**, and in relation to limited shelf life of service requests before re-checking takes place. Review how, and how well, the system and process encourage **accuracy of information completion** e.g. extent of field validation, including during testing, and guidance for system users.	Reduced	
Privacy and confidentiality procedures are not in place where they are needed	(see PIA question 13) Review and take forward appropriate action in relation to **privacy and confidentiality requirements on staff** who may have access to the asset and its data e.g. system supplier and their third party server host, and internal staff in ICT. Following review by ASC Information Governance the provisions within the system supplier’s Terms and Conditions to be used are considered completely adequate, no changes are needed.	Reduced	Confirmed
Access to information is not appropriately controlled	(see PIA question 14) **Access Control Policy** to be developed, support will be needed from IM&T and possibly ICT.	Reduced	
Access to information is not appropriately controlled	(see PIA question 14) A decision will be needed to determine what the **timeout** of the system should be set at, taking into account usability and security. Advice from our ICT security expert is that, given the data sensitivity and nature of the system, we might need to be looking at something in the region of 10 minutes, similar to an on-line banking site. Current plans are to use a 10-15 minute timeout during the testing phase, to look at	Reduced	

	the usability and business impacts of this approach.		
Records are not destroyed after the agreed retention period	(see PIA question 16) Processes need to be developed to make sure that the appropriate **contractual records in relation to each care package are retained outside of ECB** (e.g. in CIS) as appropriate in line with the contract retention period.	Reduced	
Appropriate information sharing and / or data processing agreements are not in place	(see PIA question 18 and 19) Assets or part of them are shared with other organisations. Work with the ASC Information Knowledge Management Team (Louise Whitworth) to make sure **data sharing / processing agreements** are in place where they are needed. Following review by ASC Information Governance the provisions within the system supplier's Terms and Conditions to be used are considered completely adequate, it is very clear that the contractor is the data processor and their obligations as such are clearly documented. No changes are needed.	Reduced	Confirmed.
Contingency plans and back up policies are not in place or appropriate to manage the effect of an unforeseen event.	(see PIA question 26) The **server host does not provide a failover to alternative data centres in the event of a major disaster** that rendered the system unavailable for some reason. This could be provided for a substantial additional charge. Following discussions ASC confirmed that given this was not something to be pursued, as the system was not business critical and it should be possible to use internal business contingency plans for a period of time if this was needed. The Project Board approved this approach at their August 2015 meeting.	Accepted	Confirmed
Contingency plans and back up policies are not in place or appropriate to manage the effect of an unforeseen event.	(see PIA question 26) ASC to review their **business continuity plan(s)** in order to define the process that will be taken by CCC and external providers in the event of an unforeseen event that means the ECB system cannot be used or accessed for a period of time.	Reduced	

Section D: Sign off

Who has approved the risks involved in the project and what solutions need to be implemented?

………………………[Mick Ward, Head of ASC Commissioning] ……………………………………………….……….

Who is responsible for integrating PIA outcomes back into the project plan and updating any project management paperwork?

……………………… Yvonne Roberts / Helen Gibson and Georgia Young ……………………….…………………….

Information Compliance Officer Approval

Name:……………………Louise Whitworth ……………………………………………………………….

Title:………………………Information Compliance Officer, Adult Social Care…………………

Signature:……

Date:…….

[approved and signed version 1.0 on 15 July 2015, and version 2.0 on 20 October 2015]

Glossary of Useful Terms

Item	Definition
Access Control Policy	An Access Control Policy outlines the controls placed on access to information, most commonly stored in a computer system. This can include permissions such as create, read, edit or delete. Permissions to information are usually based on an individual's job role. This is known as Role Based Access Control (RBAC). For the purposes of this document assurance is required showing consideration has been given to access to information, that this has been documented and will be monitored.
Data linkage	Data linkage refers to a merging that brings together information from two or more sources of data with the object of consolidating facts concerning an individual or an event that are not available in any separate record
Data matching	Data matching is the process by which the data held on a computer system or, manual filing system, are compared electronically with other data held on the same computer system, or on another computer system. Comparing data in this way may reveal inconsistencies and is sometimes used for the purposes of identifying indications of fraud.
European Economic Area	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Information Assets	Information Assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities.
Personal Data	This means data which relates to a living individual which can be identified: a) from those data, or b) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Personal Sensitive Data	This means personal data consisting of information as to the: a) racial or ethnic group of the individual b) the political opinions of the individual c) the religious beliefs or other beliefs of a similar nature of the individual d) whether the individual is a member of a trade union e) physical or mental health of the individual f) sexual life of the individual g) the commission or alleged commission by the individual of any offence h) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep record longer than the recommended minimum period, it can vary the period accordingly and record the decisions and the reasons behind.
Usable Audit Trail	The ability to audit / check if a record / information has been edited, read, deleted, by a particular individual, at a particular date and time.

Appendix A: Adequacy, relevance and necessity for the collection of personal and/or personal sensitive data for this asset – Electronic Care Brokerage

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

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

- More than one of these is met, focus is on use of consent.

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

- Our focus is on the use of explicit consent in schedule 3

(For more information regarding Schedules 2 & 3 please contact your directorate InCo or further information can be found on the Information Commissioners Officer website http://ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing)

Have you identified the purpose of the project?

- Yes.

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

- Service users and carers - During the assessment process and support planning. See later.

Will the Fair Processing / Privacy Notice need amending?

- This has already been done. The current Fair Processing Notice (as of July 2015, Information Sharing.pdf), was updated for spring 2015 and on the second page makes reference to information sharing with providers.

Have you established which conditions for processing apply?

- Our focus is on the use of consent in schedule 2 and explicit consent in schedule 3.

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?

- Service users and carers - during assessment process and support planning process.
  Calls taken via the Contact Centre in relation to home care referrals include content about information use and sharing by recorded message and then via an operative that asks

whether they consent, this is recorded using a consent form (these have recently been updated to specifically include providers, were developed to go live in April 2015 and are in line with the Care Act changes).
If the first assessment of the service user is in person by a social care operative information use and consent is also discussed and the user is also given a copy of the notice and form and asked about consent, and the social care operative makes sure this is recorded in writing.
– To review whether additional or revised guidance needs to be provided to assessors and care managers regarding how the service users' and carers' data will be used and what to tell them.

- If consent is withheld ASC would not share the information and consequently may not be able to put the service in place (individual would need to obtain the services themselves.)

<u>Principle 2</u>

Personal data shall be obtained only for one or more specified 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?

- To review and confirm.

Have you identified potential new purposes as the scope of the project expands?

- No – but this will be kept under review.

<u>Principle 3</u>

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?

- To be determined as systems and processes are further developed.

Which personal data could you not use, without compromising the needs of the project?

- To be determined as systems and processes are further developed.

<u>Principle 4</u>

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?

Once the brokerage process has been completed, information in the system will not be changed or amended unless there is a new brokerage request. Any changes to service user information will be made via CIS.
CIS is a record system where information needs to be updated. The ECB asset is a brokerage system so offers only a snapshot of what was brokered out. Change requests manage the

updating of information, otherwise there is no expectation that it will be current / live information.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

- By checking with them directly, e.g. data gathered about service users or carers during assessment, care planning and review should be checked by the assessor and/or care manager and/or home care provider with the service user and/or carer.

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes

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

- ASC have advised that the retention period for all records is 6 years from cessation or termination of the contract, in line with legal contract retention periods. This refers to the date of the termination or completion of each brokered care package within the new system.
- However, ASC's intention is that the system is for brokerage purposes only, and that the contracts for each care package offer and acceptance that are generated by the system will themselves be stored separately – details to be confirmed.
- Where additional data is on the system that may be subject to other retention schedules it will be a duplicate record e.g. uploaded by Access and Care from EDRMS, or present on CIS. In addition if a provider uploads content that needs to be retained in such a way, e.g. from a review of needs, Access and Care will make sure it is also held on their case management system.

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

- The preferred supplier has confirmed that for additional costs they can run on demand purges to archive records over an agreed age, or delete attachments from them.
- The preferred supplier's ECB system will archive records after 7 years inactivity, and information on asset destruction is noted below. Current contracting plans with the supplier are for up to 3 years.
- Following consideration by Information Governance the costs associated with developing the system to deal with the earlier archiving and/or destruction of records and addition of disposal rules do not appear to be worthwhile, as nothing will need to be destroyed within the period we will be using the system. Should a decision be taken to keep the system longer i.e. closer to 7 years, we will need to review this.
- In addition, for future commissioning of a brokerage system the essential requirements for disposal and destruction of information will need to be included in the specification.

<u>Principle 6</u>

Personal data shall be processed in accordance with the rights of data subjects under this Act

Will the systems you are putting in place allow you to respond to subject access requests more easily?

- Yes. Data will be stored electronically rather than on paper (at present) making it quicker to access.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

- Not applicable.

<u>Principle 7</u>

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?

- Yes – see tender documentation for ECB contract. Also we have worked with ICT colleagues on security elements, and follow-up questions with the preferred supplier to be satisfied about security issues. The ECB system was developed in response to issues with security risk of current practices e.g. emailing and faxing sensitive personal data.

- OCC is accredited to:
  - ISO27001 Information Security Management Systems.
  - ISO27002 Code of Practice for Information Security Management.
  - BIP0009 Code of Practice for Legal Admissibility and Evidential Weight of Information communicated electronically.
  - GCSX Co-Co Government Connects Code of Connection

- User account management
  - The system allows LCC administrators to manage user accounts in the system
  - The last log-in date/time of users is logged.

- Password Policy
  - Each authorised person will have their own identifying account with username and password used to connect to the system.
  - Access to administrative information and functionality (for both Local Authority users and Service Provider users) is restricted to personnel authorized explicitly by the Local Authority identified by username and password entered via a secure log-on process.
  - Measures are in place to lock user accounts should the log-on process repeatedly fail for a particular account (number of attempts configurable).

  - Accounts will be logged-out automatically after a period of inactivity (time configurable and as requested by LCC).
  - Best practices are used in the random generation of initial passwords.
  - The system can enforce that passwords are changed on first use
  - Passwords are masked as they are entered into the system
  - All passwords are encrypted during transmission and while in storage at Rackspace.

- Password Strength
  - This is configurable as required by LCC as follows
  - The policy can be set to accept minimum number of characters in the password
  - The policy can be set so that the password requires a minimum number of non-alphanumeric character (e.g. $%&)

- Areas where the password policy does not reach internal LCC policy levels
  - Password changes are not enforced every 90 days
  - The system does not ensure that passwords are not reused within 20 changes

- Two-factor authentication
  - Because of the nature of the sensitive and personal information that will be stored in the system it is necessary to provide a further level of security by way of two-factor authentication
  - The preferred supplier has stated that they will provide this through the development of their own in-house service with a fixed monthly price per user, which would provide a defined upfront cost
  - Analysis undertaken of user devices, and also a full cost analysis points to delivery of tokens via SMS as being the preferred option
  - The preferred supplier has stated that the users IP address **cannot** be used to determine if single factor or two factor can be used (i.e. allowing for internal users on the corporate LCC network to log in using single factor). They do have a facility to use the ‘type’ of user to do this (e.g. LCC Staff, External Provider), but LCC consider this inappropriate and so will use two factor for all users, regardless of their designated type.
    - If a username/password of an LCC employee was maliciously stolen, the system could be accessed from any device with single factor, leading LCC to the conclusion that two factor will always be mandated.

- Security of data in transit
  - Data in transit is secured with HTTPS and is encrypted using the Transport Layer Security (TLS) protocol (which is a more secure successor to Secure Sockets Layer SSL).
  - OCC will require a domain name and certificate to be provided by council, and can support any strength and version that LCC require.

- Security Penetration testing

  - Other authorities using the same system supplier have already undertaken penetration testing of the system, including testing against the OWASP Top 10 and any key issues arising have been resolved by the supplier.
  - The most recent customer penetration testing report from Durham Council has been provided to LCC and OCC have stated that all significant risks that were identified were addressed within two days.
  - The preferred supplier undertook its own penetration testing in August, and the report and resulting actions was provided to LCC in September. The supplier has confirmed that they have resolved all issues raised as high or medium risk. Review of a subsequent penetration test from another authority did not highlight the same risks, and was considered satisfactory .
  - LCC plan to undertake periodic penetration testing when the system is live.

- Secure Integration to CIS
  - No integration is proposed for the initial phase of the deployment
  - LCC will need to work with the supplier at the appropriate time to determine how and whether the ECB can be securely integrated with CIS (currently the integration requirements have not been defined and so this work can not yet be undertaken).

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

- To be determined as new processes and systems are further developed. Workforce development workstream established to lead on this area – Gill Dickinson is the work stream lead.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of data

Will the project require you to transfer data outside of the EEA?

- No. This issue is included in hosting agreement for electronic care brokerage contract.

If you will be making transfers, how will you ensure that the data is adequately protected?

- Not applicable.