DERBYSHIRE
County Council

Information Security Document

ICT Hardware Disposal Tender Privacy Impact Assessment

Version 1.1

Version History			
Version	**Date**	**Detail**	**Author**
0.1	01/08/17	First Draft	[redacted]
0.2	08/08/17	Second Draft	
1.0	28/09/17	Final Version – step 6 completed following sign-off	
1.1	08/02/18	Step 6 dates updated	

CONTENTS

Contents	Page
Section 1 - Privacy Impact Assessment Screening Questions	4
Section 2 - Privacy Impact Assessment:	
- Step one: Identify the need for a PIA	5
- Step two: Describe the information flows	6
- Consultation requirements	6
- Step three: Identify the privacy and related risk	7
- Step four: Identify privacy solutions	8
- Step five: Sign off and record the PIA outcomes	10
- Step six: Integrate the PIA outcomes back into the project plan	10
Section 3 - Linking the PIA to the Data Protection Principles	12

Section 1 - Privacy Impact Assessment Screening Questions

Will the project involve the collection of new information about individuals?	NO
Will the project compel individuals to provide information about themselves?	NO
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	NO
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	NO
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	NO
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	NO
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	NO
Will the project require you to contact individuals in ways that they may find intrusive?	NO

Although none of the questions above can be answered ‘Yes’ for this project, a PIA is still necessary – see below.

Section 2 - Privacy Impact Assessment

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal.
Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Derbyshire County Council has a requirement to dispose of all surplus ICT equipment in compliance with UK and European Legislation. An open tender will be carried out under usual procurement procedures to identify the most suitable supplier to provide a collection and disposal service.

See the Business Case for full details - https://edrmlive/livelink/llisapi.dll/properties/78133628

Responsible and traceable disposable ensures that sensitive data is not accidentally supplied to individuals. However, there is always a risk, albeit low, that Council equipment which contains data is not appropriately disposed of, hence the need for a PIA.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

There is no data flow as such. However, equipment and items which contain data and which cannot be shredded in-house are taken off site by the disposal company for destruction at their treatment site. The process is as follows:

1. Once a collection has been arranged the contractor parks their vehicle in the agreed location at County Hall and signs in at the collection point - operatives must show proof of identity;
2. The contractor collects the items for disposal and loads them into their vehicle;
3. Council staff witness the collection and check the equipment off site using a detailed inventory of the items being collected;
4. The Council and the contractor both complete a Waste Transfer Note / Hazardous Waste Consignment Note as appropriate, which contains a description of the wastes collected and the relevant waste codes;
5. Two Council staff follow the contractor's vehicle to their treatment site and witness the destruction of the items;
6. The contractor subsequently sends the Council a file containing as a minimum the manufacturer, model, serial number and asset number for each item removed from site as confirmation that the items have been destroyed.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

The project team includes representatives from the Asset Management Team, the Server Team, Internal Audit, IT Security and Waste Management, all of whom have contributed to the tender documents to ensure that the Council's needs are met, including data security requirements.

See the project Stakeholders and Communication document for full details - https://edrmlive/livelink/llisapi.dll/properties/74754780

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.
Section 3 can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Equipment and items that contain sensitive data are not destroyed and the data is accessed by unauthorised persons.	Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.	Breach of Principle 7 of the Data Protection Act.	Financial and reputational damage. Legal action could be taken against the authority and possibly a substantial fine.

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Equipment and items that contain sensitive data are not destroyed and the data is accessed by unauthorised persons.	Continue to follow Council policy to shred devices containing data in-house. Reject as non-compliant tenderers without the appropriate levels of insurance or an Environmental Permit, Waste Carrier Licence, ADISA certification (or equivalent), or T11 certification. Include a requirement that tenderers explain the contingency arrangements they would implement to ensure devices containing sensitive data are held securely in the event that the destruction of the items cannot be completed due for example to a	Reduced	The project team believes all reasonable steps will have been taken to ensure that a suitable supplier is chosen and that the disposal procedures will continue to mitigate against sensitive data being accessed by unauthorised persons.

	vehicle breakdown or failure of plant and machinery. Carry out due diligence via a site visit to the highest scoring tenderer's treatment site to validate their tender responses. Once the contract has been awarded, items that cannot be shredded in-house to be accompanied by two Council employees to the disposal company's treatment site and the destruction of the items to be witnessed. The disposal company to provide documentation to the authority confirming that the items have been destroyed. Carry out rigorous contract management to ensure that the supplier continues to meet the authority's requirements throughout the term of the contract. The risk will be added to the departmental risk register and the secure treatment procedures will be submitted to the Information Governance Group for review.		

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
As step 4	As step 4	

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Continue to follow Council policy to shred devices containing data in-house.	Ongoing	Asset Management Team
Reject as non-compliant tenderers without the appropriate levels of insurance or an Environmental Permit, Waste Carrier Licence, ADISA certification (or equivalent), or T11 certification.	Complete	Corporate Procurement
Include a requirement that tenderers explain the contingency arrangements they would implement to ensure	Complete	Project Team

devices containing sensitive data are held securely in the event that the destruction of the items cannot be completed due for example to a vehicle breakdown or failure of plant and machinery.		
Carry out due diligence via a site visit to the highest scoring tenderer's treatment site to validate their tender responses.	Complete	Project Team
Once the contract has been awarded, items that cannot be shredded in-house to be accompanied by two Council employees to the disposal company's treatment site and the destruction of the items to be witnessed. The disposal company to provide documentation to the authority confirming that the items have been destroyed.	New contract to commence 01/04/18	Asset Management Team / Server Team
Carry out rigorous contract management to ensure that the supplier continues to meet the authority's requirements throughout the term of the contract.	Ongoing	Corporate Procurement – Contract Manager
Add the risk to the departmental risk register.	Complete	
Submit the secure treatment procedures to the Information Governance Group for review.	Ongoing	Asset Management Team

Contact point for future privacy concerns
Carol Brown

Section 3 - 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 DPA 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** **b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**	
Have you identified the purpose of the project?	Yes
How will you tell individuals about the use of their personal data?	n/a
Do you need to amend your privacy notices?	No
Have you established which conditions for processing apply?	n/a
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?	n/a
If your organisation is subject to the Human Rights Act, you also need to consider:	
Will your actions interfere with the right to privacy under Article 8?	No
Have you identified the social need and aims of the project?	n/a
Are your actions a proportionate response to the social need?	n/a

Principle 2 - 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?	n/a
Have you identified potential new purposes as the scope of the project expands?	n/a

Principle 3 - 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?	n/a
Which personal data could you not use, without compromising the needs of the project?	n/a

Principle 4 - 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?	n/a
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	n/a

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?	n/a
Are you procuring software that will allow you to delete information in line with your retention periods?	No

Principle 6 - 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?	n/a
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	n/a

Principle 7 - 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
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	None

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	
Will the project require you to transfer data outside of the EEA?	No
If you will be making transfers, how will you ensure that the data is adequately protected?	n/a