Privacy Impact Assessment
Hybrid Mail letter processing

Version	Date	Detail	Author
1.0	2/10/17	Draft for comment	

Step one: Identify the need for a PIA

The introduction of Hybrid Mail for users – a process where any printed letters generated by users are sent directly to a fulfilment house to print, add to an envelope and post - will provide many efficiencies. These include

- Reduction in postage cost
- Reduction in stationery cost
- Reduced requirement to maintain expensive equipment in the Derbyshire Business Centre
- Operational efficiencies, for example, a user can carry out the process from their desk rather than visit the printer, envelope store or the post box.
- Quality of output – it is not possible to hand write on envelopes, typing the address and the address checking should drive forward 'cleaner' address data, and better customer perception
- A secure transfer of letter information during the process.

As with the current letter fulfilment process, including bulk Hybrid Mail processed by Derbyshire Business Centre, the new system will hold information about individuals and businesses who interact with Derbyshire County Council, and may include contact details of employees. Some of the data may be sensitive.

Taking into account:

- personally identifiable data is held on any letters sent
- the sensitivity of some of the letters
- the new printing process will be externally hosted/Cloud based, rather than fulfilled on site by individual users as currently.

Comprehensive steps have been taken throughout the project to identify and minimise the privacy risks of the new system and these are captured in the Privacy Impact Assessment.

DRAFT

Step two: Describe the information flows

Individuals affected by the new system will include:

- Any individual that is sent a letter from Derbyshire County Council. These could be employees, job applicants, individuals receiving care, individuals receiving a chargeable service.
- Any business that is sent a letter from Derbyshire County Council. These could be providing a service, receiving a chargeable service.
- Any employee whose details appear on letters sent from Derbyshire County Council

The key flows of information are summarised below:

Letter is generated by the user

Letter documents can be generated electronically on a user device/ pc containing recipient details

a) from a template - these may automatically include the recipient name and address on the letter. An example of this is an Invoice template generated from our transactional system
b) by typing details in manually

Letter is sent to remote site ready for printing

Once the letter is open on screen, the printer is selected. The user is required to login to the Opus Trust printer each day with username and password.
The locally installed print driver is used to securely transfer print files over the Internet to Opus Trust.
The print driver requires that the user authenticate with the Opus Trust web portal.
The data transfer session is encrypted using TLS and the HTTPS protocol.
The associated certificate installed on the web service has been provided by a 3rd party certificate authority.
The web service is logically located within Opus Trust Internet DMZ, the print files are stored within their internal production segment.

Letter is printed at Opus Trust
All letters are stored and processed on dedicated production systems with access restricted to the Opus Trust IT infrastructure and implementations teams.

Physically, all server hardware and networking equipment is located within a secure server room at Opus Trust production facility in Leicester. Only the IT Infrastructure team has access.
The room is secured by means of a swipe card access control system and CCTV.

Files approved for printing are retained by Opus Trust for a period of 14 days before being automatically purged from their systems.

Note that users may choose to keep a copy of the letter on a shared drive. Training will ensure that these copies will be deleted according to DCC policy.

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 suppliers were consulted and involved from the inception of the project, through the initial development of procurement specifications, through to the ongoing implementation. Consultations within DCC include ICT services, the ICT Security Team and Contract Management, Procurement, Audit, and Legal Services.

The Security Team were consulted on the areas of risk which should be fed into the risk register.

The Council's Information Governance Group have been consulted on the information security implications of the project.

As part of the Project Governance process, the Project Board have identified and monitored risks through the project risk register, including those relating to personal data transferred to Opus Trust.

Key requirements have been at every stage of procurement and implementation that the solution is technically robust, protects data integrity and holds data securely, and complies with the Council's existing standards. Opus trust have the following accreditations:
ISO 22301: 2012
ISO 14001: 2015
ISO 9001: 2015
ISO/ IEC 27001:2013

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.

Annex three can be used to help you identify the DPA related compliance risks.

The project Risk Register developed and monitored through Project Board identifies risks associated with information security.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Data not kept or sent securely – disclosure of information during the process	Psychological distress of personal data being disclosed	Non-compliance with ISO (or equivalent) Non-compliance with code of practice, DPA	Reputational damage and loss of public trust Financial penalties Regulatory action Loss of employee trust
Data retained for longer than is appropriate	Letters retained for longer than needed	Non compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation e.g. Employment	Resource implication of storing/processing data for longer than necessary. Negative impact on organisational effectiveness and efficiency of processes.

		equalities legislation	

Step four: Identify privacy solutions

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

General
The council has ISO27001:2013 certification and has established an information security management system in accordance with the requirements of ISO27001 and ISO27002 code of practice for information security controls.

The council requires the supplier to provide a level of information security assurance for Council and personal data compliant with current Data Protection Legislation and Information security best practice.

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?
Data is not retained within the system securely.	Contract requires supplier to comply with Council security policies including Information Security Policy, Third Party Connection policy and Data Protection and Storage media handling policy, and ISO27001 certificate or equivalent.	Supplier (processor): risk is eliminated User (controller): risk is reduced	

DRAFT

	Organisational information security policies and practices in place, and guidance for managers – these will be reinforced during training.		
Letters retained for longer than required.	Automatic deletion of records within system to comply with the data retention schedule requirements. Managers trained in information security as part of the training process.	Supplier(processor): eliminated	
Inappropriate access by individuals to sensitive data leading to misuse of data	Technical and administrative measures in place to prevent misuse of data e.g. access controls based on user login. Requirements defined in contract with supplier, which will be audited/tested within the system, Council's stringent password policy complied with. Derbyshire County Council policies on information security. ie personal logins should not be shared	Eliminated	

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
The risks above have been identified by stakeholders as part of the development of the System requirement document, and reflected in the contract with the supplier and implementation plan.	The approved solutions above have either a) been identified by stakeholders as part of the development of the System requirement document, and reflected in the contract with the supplier or b) identified as part of implementation and incorporated into the implementation plan.	

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
Project Board to review PIA outcomes and ensure implementation plan reflects the approved solutions.	On implementation of the system	Project Board

Contact point for future privacy concerns

DRAFT

Annex three

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?

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

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

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?

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?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

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?

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

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?

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

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?

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

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?

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

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?

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

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?

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

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?

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