

Gifts Are Us Privacy Impact Assessment

1. Project summary: New Online Service Offering

This is a new online offering, so some new systems are required. Products will also need to be listed on our existing website. New online invoicing will be required, while we can also continue to use our existing invoicing processes for manual invoicing.

The purpose of the change is to develop an online offering, to customers who would like to buy goods through extending the functionality of our website. The benefits would be that we could expand our product sales and give customers the ability to purchase online.

The main stakeholders include employees of Gifts Are Us Company (administration, marketing, management) and customers.

2. Scope of the PIA

2.1 Scope

Current administration procedures will be expanded upon and there will be two new It systems included. These include:

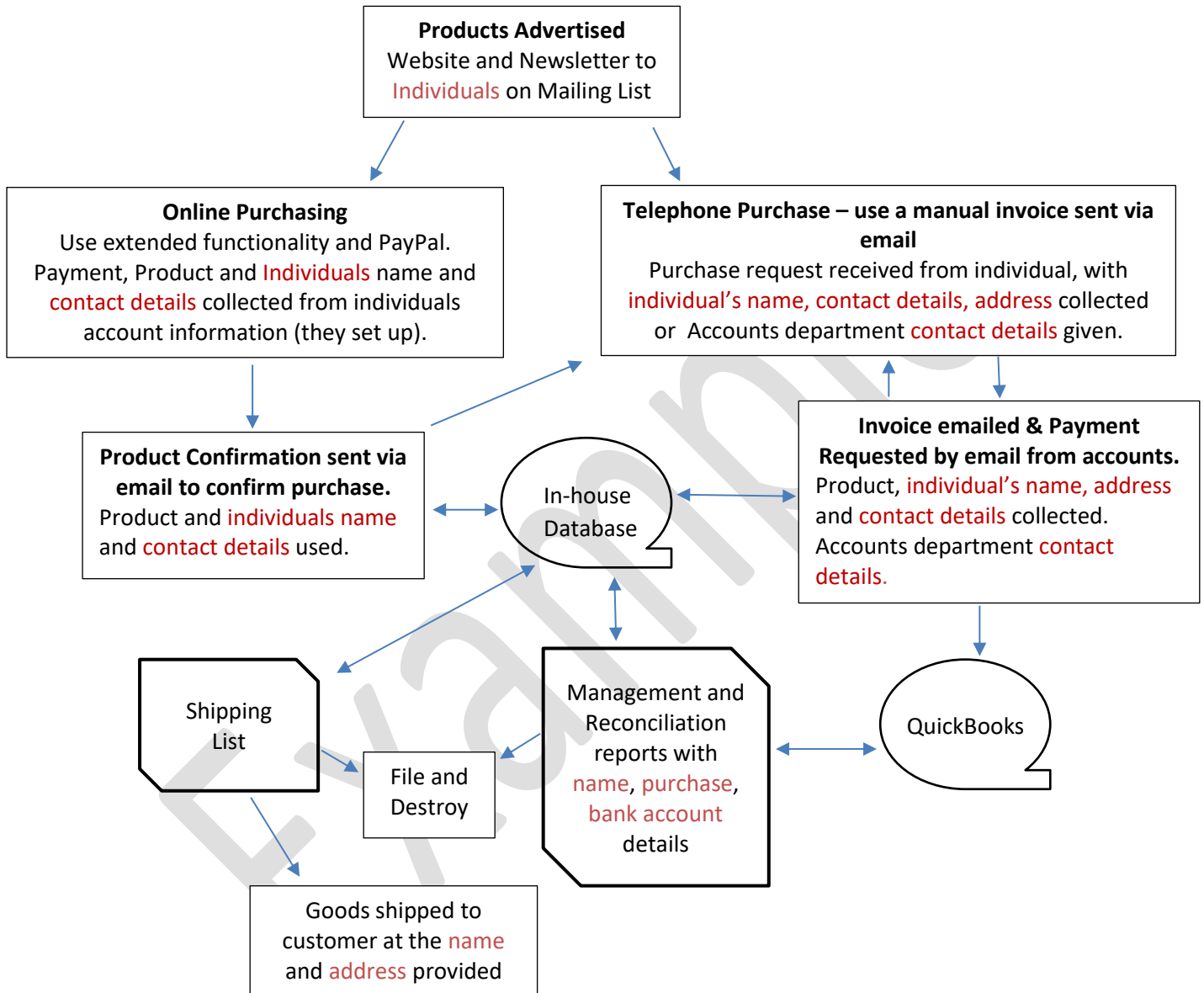
- New shopping cart functionality to purchase products
- New payment functionality and PayPal option for payments
- expansion of the use of our in-house database to record personal information, billing information and purchases
- Order fulfilment and processes required to ensure information is not printed out or duplicated
- This PIA requires the checking of data handling and contractual information regarding third parties. However, does not include a physical visit to ensure the controls are as outlined in the contractual agreement.

2.2 The process

This PIA was conducted internally by Jane Boggs (Project Manager) and in discussion with advice given from the heads of our IT, marketing, operations and sales departments (prior to deciding on the new systems being embedded into the company and implementation of the new processes).

3. Personal information

The following process shows the personal information being collected and the flow of information in the new system. If not otherwise detailed, information is passed between systems via email.



All information collected is collected by the individual who is authenticated through their account access. Information will only be used for the purposes in which it has been collected and a privacy notice will be required to communication the information collected and what it will be used for, along with who will have access to that information. An additional consent form will be used to allow users to opt into marketing emails, with each email having an ongoing option to 'opt out'.

4. Privacy assessment

Assessment of potential risks and possible mitigations to reduce or manage adverse effects							
Principle 1 : Purpose of collection of personal information							
Ref. no.	Purpose of collecting the information	Description of the risk	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R01.	Purchase and sending of products	Information becomes out of date	Risk of purchases being lost or not going to right person.	As informed by individual or company	Minimal, but ongoing as people move.	Details will need to be confirmed with each purchase	Minimal – mainly financial losses and consumer inconvenience.
Principle 4: Manner of collection of personal information							
Ref. no.	How you are collecting personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R02.	Through online portal or manually	Maintaining accurate records	Reputation Risk, unwanted exposure	Ensure information is checked with each transaction.	Ensuring any returns or 'no deliveries' are recorded. Remediate data.	Remediate data and try to contact person. Get telephone number on purchase.	Nil
Principle 5: Storage and Security of personal information							
Ref. no.	How you are storing and securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards

R03.	Info sent to 3 rd party provider	Data secured & held in country with 'Adequacy status'	Contract and bank information hacked	Contract and secure upload screens	Reduced, however reliant on honesty and reputation of supplier	Find out country information is stored in.	Yes – company could be hacked and data exposed.
------	---------------------------------------------	-------------------------------------------------------	--------------------------------------	------------------------------------	----------------------------------------------------------------	--------------------------------------------	-------------------------------------------------

5. Risk assessment

This section describes the privacy risks you've identified through the PIA process and how you propose to mitigate and manage those risks. It can be useful to link this back to the privacy principles to show why these risks and the proposed actions are relevant.

Categorise your proposed actions

In some cases, it may be helpful to categorise these actions into areas such as:

- governance
- people
- process
- technology

Categorising the proposed controls in this way helps to define where within the organisation they will be managed.

Add a narrative summary of your risk assessment and options for mitigating those risks here. Alternatively, attach a separate risk assessment document. Document the risks in line with any existing risk management processes your organisation has – it will be more efficient than trying to run a separate process.

6. Recommendations to minimise impact on privacy

Summarise the recommendations to minimise the impact on privacy based on your risk assessment