Public

Information Security Document

Prepaid Account System Privacy Impact Assessment

Version 0.3

Version History			
Version	**Date**	**Detail**	**Author**
0.1	30/06/17	First Draft	
0.2	29/12/17	Second Draft	
0.3	05/01/17	Third Draft – Remove reference to employment legislation	

ADULT CARE

PRE-PAID ACCOUNT SYSTEM

FOR DIRECT PAYMENTS

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).

The aim of the project is to provide a pre-paid account solution for Direct Payment users. Please see Cabinet report of 15 December 2015 for more detail.

The benefits will be the ability to:

- Create new accounts online
- Directly view Direct Payment transactions through the bank accounts
- Monitor transactions electronically
- Suspend accounts
- Recoup contingencies
- Recover balances on closed Direct Payments
- Close accounts

The main advantages to individuals will be removing the need to submit paperwork for monitoring purposes and the provision of a Customer Services to support clients in using their accounts, making payments etc

Currently users have to submit full details of all transactions on their Direct Payment bank accounts, but this system will allow real time access and gives us direct access to add or remove monies from the account. Due to this increased level of access it is felt that a PIA is required.

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.

All personal information regarding the client will already be available in Frameworki (the Electronic Social Care Record system, due to be replaced by Mosaic in 2018).

A new workflow has been added to Frameworki to manage the new prepaid accounts. The steps involved are:

- The Direct Payment Social Worker forward a copy of the completed Direct Payment Agreement (DPA) to the Direct Payment Finance Team. This agreement includes details of the clients name, address and DoB and also the same information for any person approved to provide support for the client
- An account is created within the Prepaid Account system
- The SAP Vendor record is added/updated with details of the new account number and sortcode
- A purchase order is created in Frameworki and a payment cycle run. These payment details are transferred via interface to SAP and a BACS payment is made into the new account, followed by further scheduled payments every four weeks
- The provider creates a debit card which is sent directly to the client or their approved support person
- The card is activated via the Interactive Voice Response (IVR) system or by calling Customer Services
- The client can then make payments to care providers vis bank transfers, standing orders, direct debits etc

In addition, the system has a full range of reports and alerts that can be accessed by the Direct Payment Social Worker Team and Direct Payment Finance Team.

Reports available are:-

- Load Report
- Card Activation Report
- Card Closure Report
- Card Created Report
- Card Replacement Report
- Card Status Report
- Transaction Report

- Direct Debit History Report
- Payment Request Report
- Reconciliation Report

Alerts available are:-

- Card is blocked
- Email address has been amended
- Failed load
- More than x POS/ATM declines
- POS/ATM transactions outside list of countries
- Balance above x value
- Balance below x value
- POS transaction above £x
- X POS/ATM transactions attempted in x minutes
- New Direct Debit set up
- New Standing Order or Bank Payment Request set up
- No spend/debit activity in x days
- No spend on card for x days

Other than details of the actual bank account and their associated transactions there is no intention of holding any additional personal information not already held in Frameworki.

If all Direct Payments users transferred on to this system then approximately 1800 individuals would be affected.

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.

Stakeholders consulted and involved from the inception of the project, through the initial development of procurement specifications, through to the ongoing implementation include ICT services, Corporate Finance and Audit.

The Corporate Finance team were consulted on the tender specification to ensure that the Data Protection and Banking Standards were up-to-date.

Throughout the project key requirements have at every stage of procurement and implementation have been that the solution is technically robust, protects data integrity and holds data securely, and complies with the Council's existing standards, e.g. ISO 27001 and Data Protection act.

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.

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation / corporate risk**
Data not retained securely – disclosure of information from system	Psychological distress of personal data being disclosed	Non-compliance with ISO (or equivalent) Non-compliance with code of practice and DPA legislation	Reputational damage and loss of public trust Financial penalties Regulatory action Loss of client trust
Individuals without the relevant permissions accessing data e.g. personal data provided on the application form, equalities monitoring data	Psychological distress of personal data being disclosed	Non-compliance with ISO (or equivalent) Non-compliance with code of practice and DPA legislation	Reputational damage and loss of public trust Financial penalties Regulatory action Loss of client trust
Misuse of information – information used for other purposes that that specified	Reduces confidence in the prepaid account system	Non- compliance with DPA legislation	Reputational damage and loss of public trust Financial penalties Regulatory action

			Loss of client trust
Data retained for longer than is appropriate	Client's information used for longer than appropriate or for new purposes, without individual's knowledge	Non-compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation	Resource implication of storing/processing data for longer than necessary Negative impact on organisational effectiveness and efficiency of processes
Consent to process personal data not collected at every necessary stage	Individuals do not understand what is happening to their data	Non-compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation.	Financial penalties Regulatory action Loss of client trust

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?**

Data not retained securely – disclosure of information from system	The system will be accessed via a secure website hosted by the system provider. The provider has confirmed that the system meets the following industry standard: Conform to all relevant Industry/Scheme Security Standards applicable to physical payment cards and include all security features required by Industry/Scheme Security Standards Process and store data (including back-up data) in accordance with the Data Protection Act 1988 Be PCI DSS (Payment Card Industry Data Security Standard) compliant when carrying out manual and/or automated processes Use application systems which store, process and/or transmit Account Holder data that are PA-DSS (Payment Application Data Security Standard) compliant and which are certified with the Payment Card Industry Security Standards Council (PCISSC)	Reduced – reliant on workers following approved procedures	Yes

	Maintain data security and integrity in accordance with the ISO27001:2013 standard or equivalent Process transactions in accordance with both the Prudential Regulatory Authority and Financial Conduct Authority regulations		
Data on registered users retained for longer than required e.g. when no longer an ‘active’ user	Registered users accounts to be reviewed regularly to ensure they are still required	Eliminated	Yes
Financial Data on clients retained for longer than required	Work with the system supplier to develop an option to delete records within system to comply with the data retention schedule requirements	Reduced – reliant on an enhancement to the current system and manager compliance with retention schedule	Yes
Consent to process information not rigorously obtained from individuals	Consent required as part of the assessment process to be fully recorded in Frameworki	Reduced - Reliant on the operational worker obtaining and recording the required consent	Yes
Unnecessary or irrelevant data held	As part of system configuration and development it is ensured that data is only collected	Eliminated	Yes

	at the point it is needed with clear justification as to why it is required		
Inaccurate data held within the system	System designed to be as user friendly to reduce inaccuracies. Effective training for workers and support to clients to ensure the system is used in accordance with protocols and processes	Reduced – human error when entering information not eliminated	Yes
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 responsibility and job role. Effective access controls in place	Eliminated	Yes
Data stored in more places than necessary	The project approach has been that data required should be stored in the prepaid account system where required. This will eliminate the need to record client's financial and personal information on spreadsheets or databases	Reduced – relies on all users of system including managers not duplicating information	Yes

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
All the risks above have been identified as part of the development of the System and reflected in the contract with the supplier and implementation plan	The approved solutions above have either been identified as part of the development of the System requirement document, and reflected in the contract with the supplier and in the implementation of the system	Head of Finance

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
Ensuring implementation of new pre-paid card solution addresses all privacy issues	Prior to go live of system	Project Team

Contact point for future privacy concerns