DPIA – NHS Tayside Charitable Foundation

Submitting controller details

Name of controller	Shelley McCarthy
Subject/title of DPO	NHS Tayside Charitable Foundation Website

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Creation of a website for NHS Tayside Charitable Foundation is a key priority which will help to raise awareness of the funding, projects and support available.

The purpose of the charity is to improve the health of the people of Tayside however work is underway to develop a new strategy which will be central to this new online development. The key elements of the website which require a DPIA include:-

Specification	Data Collection
Develop and deliver as part of the website: Automation with donations platform of our choice – i.e. Crowdfunder/GoCardless/Just Giving	Applications in & monitoring Online donations Crowdfunding
Optimised UX (user experience) aligned with sites key objectives – 'Apply Now' & 'Donate'	Automated service which aims to reduce admin work
Document Store	Provide a space on the website where publications can be stored

A DPIA has been drafted to ensure that all risks are mitigated with regards to data collection and GDPR regulations.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The charity will collect data through the website interface where we are asking for donations and application information.

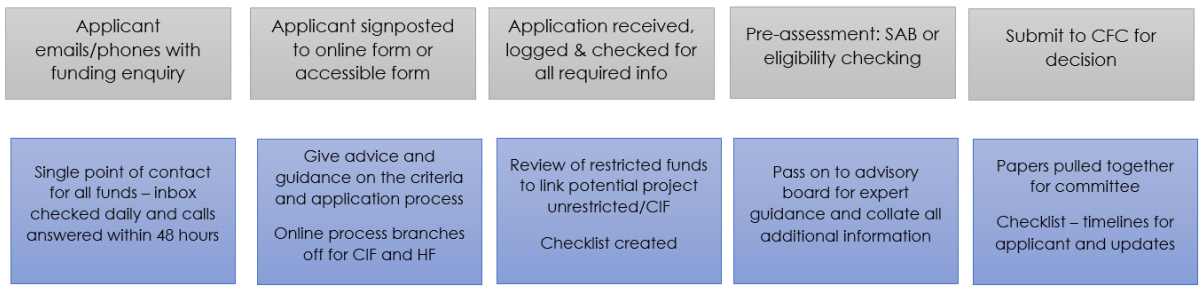
Donations – Once the donation is collected through Worldpay, the personal data will be deleted and each payment given a code for reference. This is needed for audit and transparency purposes.

Applications – Personal information is kept to a minimum on a funding application form. It is proposed to ask for a contact, email, address and phone number. As per the OSCR regulations all paperwork relating to a funding application will be kept for six years under the file retention scheme.

Contact Us – within the website there will be an option for people to submit a request for us to contact them based on their enquiry for funding or to fundraise. Once the enquiry is passed on and answered the personal details will be deleted.

To keep data collection to a minimum there will be an evolving 'frequently asked questions' section on the website to reduce direct contact. We will however ensure that our service is fully accessible and where people need a call back or to download an application there will be a facility for that.

The data will only be accessible to the team which includes 6 people throughout the following process: -

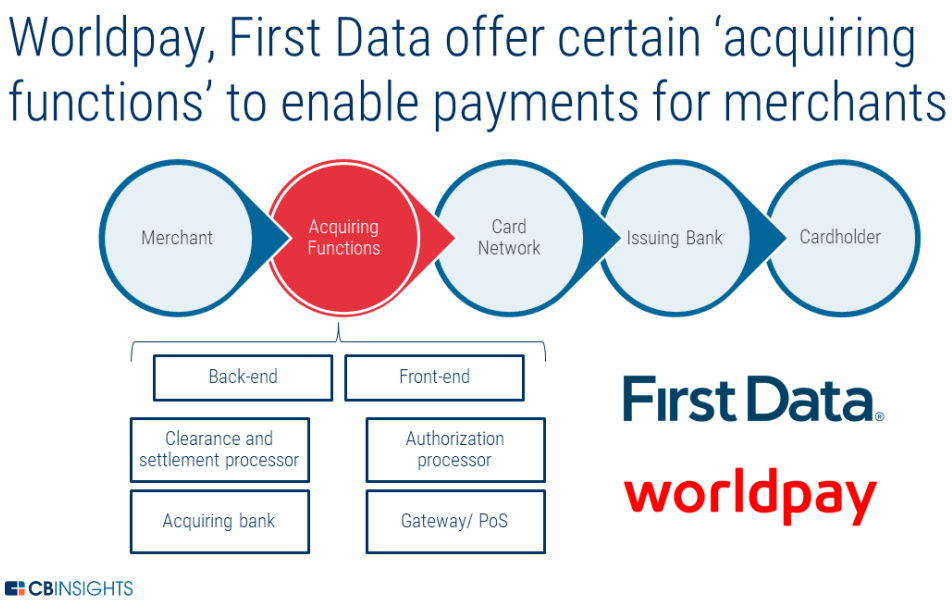


Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data

The data collected as part of the application and enquiries is: -

- Name as a lead contact
- Email address to enable a reasonable flow of information to and from the applicant
- Address to enable due diligence and fraud reduction
- Phone number for queries

For donations to the charity, there is an intermediary party 'Worldpay' used by NHS Tayside so none of the individual data is passed over to the charity. A code will be given to enable an audit trail.



Due to the nature of the charity, it is unknown when people will make donations or make an application to the charity.

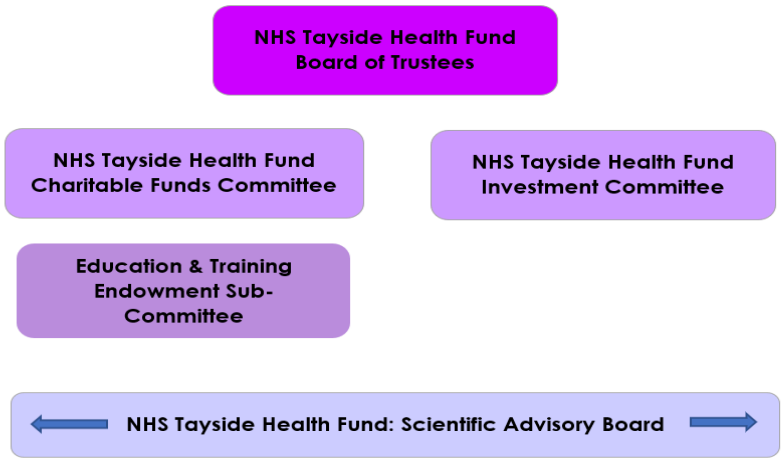
The funding applications are restricted to those operating in Tayside but donations are global.

Describe the context of the processing:

The Charity is a fund distributing organisations with a Fundraising arm. The relationship we have with our customers is that we're either giving them funding or they are fundraising for us and donating funding.

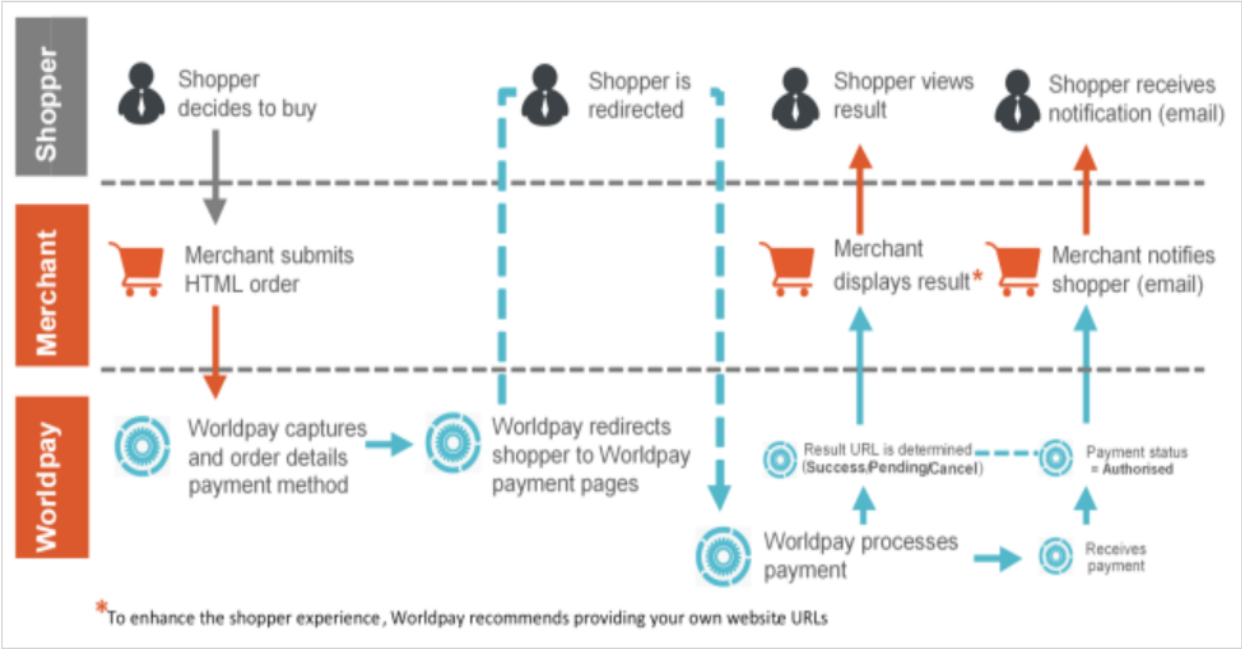
Our relationship with fundraisers is significant as we have several interactions with them while they are fundraising, including providing them with branded clothing and advising them on fundraising. They then become donors once the activity is complete and, at present, can either send us a cheque or BACS payment. This DPIA is to enable a more streamlined way for donors to give their funding to us.

Funding applicants provide us with their information so that we can process their application and seek approval from the Charitable Funds committee. We have a robust governance process in place: -



The Charity takes the risk of internet fraud very seriously. The Worldpay payment system uses state-of-the-art encryption techniques and supports the industry-leading anti-fraud systems provided by both Mastercard and Visa.

In addition, Worldpay has developed anti-fraud software which provides the customer with a sophisticated detection system designed to identify potentially fraudulent transactions. See diagram below.



Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

NHS Tayside Charitable Foundation holds endowment property and funds for purposes relating to health services or research. The Fund is funded by donations and legacies received from patients, their relatives, the general public and other organisations. The overall strategy of the Fund is to provide support to Tayside NHS Board in whatever way the Trustees consider appropriate, subject to any specified directions prohibiting such expenditure which may have been issued by Scottish Ministers.

The Charity aim to distribute and lever in funding to deliver the vision – People live better and longer lives in Tayside.

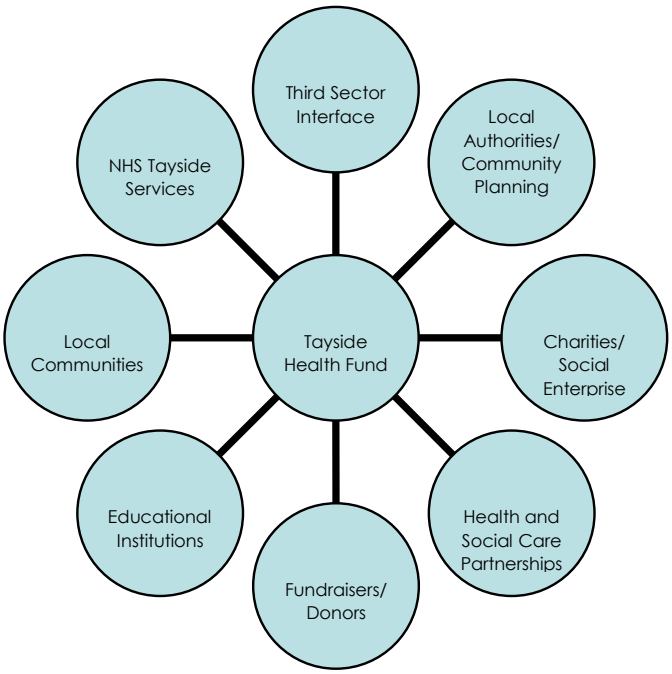
The benefits of funding projects and levering in funding is that more projects will be delivered across the area which supports the delivery of our priorities –

- Improving and supporting physical and mental Health
- Reducing substance use
- Promoting child health
- Health innovation
- Obesity and physical activity
- Environmental sustainability

Step 3: Consultation process

Consider how to consult with relevant stakeholders:

The Charity engages with local people on a regular basis through workshops and surveys. There are established networks that are available for audit and scrutiny throughout the year. There is also an internal audit department that provides scrutiny throughout the year, which is then followed up with an audit improvement plan. Current partners and stakeholders include: -



On a National level, OSCR, the charity regulator, is informed of the work underway, and the Scottish Government oversees the legislation underpinning the endowment funds.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

The charity receives donations on a regular basis and this piece of work has been developed to make the process and access safer and more streamlined. A Privacy Policy has been drafted alongside this DPIA and outlines the precautions taken to protect any data we receive. The processing of online donations will increase the funding coming into the charity and follows the good practice model developed by other endowment funds across Scotland. With the increase in online payments and transactions, the charity needs to develop this function.

At present there is no other way to collect online payments in a safe and secure manner – this project will be utilising World Pay services who have a robust compliance and counter-fraud programme in place.

To protect donors' rights, we will keep data collection to a minimum as outlined in the OSCR regulations for charities. Any personal data will be replaced by numeric codes to enable tracking.

Internally we will adopt a four-stage process:

- Profiling, evaluating, or scoring data subjects (e.g., for predictive purposes)
- Automated-decision making
- Systematic monitoring
- Processing sensitive data or data of a highly personal nature

Through this process, we will help to identify and mitigate potential risks and threats that may affect the privacy and security of individuals. Another aim is to help organisations comply with applicable data protection laws and regulations, including the General Data Protection Regulation (GDPR).

We aim to foster trust with our customers/donors or stakeholders by demonstrating our commitment to data privacy and protection. Through this DPIA process, we can also uncover opportunities to improve our data privacy practices, accountability, and governance. This

DPIA also provides us with a structured approach for assessing the impact of our data processing activities.

Step 5: Identify and assess risks **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. Risk of using an external organisation (World Pay) as an intermediary – there are limited options outwith using a company to deliver this service.	Low	Low	Low
2. Data breach of personal data	Medium	Low	Medium
3. Website is hacked	Medium	Medium	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
1	The DPIA and privacy policy have been drafted to mitigate this risk	Mitigation through governance	Limited	Yes
2	The collection of personal data will be kept to a minimum	Mitigation through collection process	Limited	Yes
3	Utilising security software as part of the website build and regular review	Mitigation through security process	Limited	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Shelley McCarthy – Charity Chief Officer 1/09/2023	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Board of Trustees	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	NHS Tayside Data Controller	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Happy to proceed		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Shelley McCarthy	The DPO should also review ongoing compliance with DPIA