This template should be used to record the DPIA process and outcome. It follows the process set out in ICO guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

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.

The aim of the project is to use database software to improve record keeping and reporting on a range of activities.

Premises management information is currently held in a variety of data folders and records such things as risk assessments, maintenance schedules, proof of appropriate maintenance of lifts and lifting equipment, contractor’s documentation, safety certificates, accident reports and so on.

These are all flat files making it difficult to easily extract information.

Similarly Clinical data on falls, incidents like drug errors and SUIs are held on either paper or digital form but rely on physical processes to ensure that appropriate procedures and reporting routes take place. While this has not currently caused any material problems there is an inherent risk in relying on human intervention (someone could fall ill and leave a process incomplete with no-one the wiser). It is intended that developing robust workflows that are automatically triggered by data input will further de-risk the system and also allow much easier data analysis to be performed as part of our internal control and audit systems.

Because some of the data held on this new database may contain personally identifiable information it was determined that a DPIA was necessary.

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?
Data will be collected by Clinical and Premises staff and input into the Vantage database. This will include scanned documentation as appropriate. Data will be sourced from patient interactions as well as supplier documentation. We will not be sharing data with anyone unless there is a justifiable need to do so ie reporting a SUI or RIDDOR reporting or ICO data breach reports. Any data shared will be the minimum required and anonymized where appropriate. We do not believe that any of the processing could be described as high risk.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Data would not include special category or criminal offence information. Where data is of a clinical nature its management and disposal will follow NHS guidelines and our Records Management Policy. Premises data such as safety certificates will be retained indefinitely.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The individuals may be Patients, staff or volunteers. Premises data is about corporate entities and is simply a record of transactions. Non clinical accident information does contain personal details as is necessary for adequate safety records to be maintained.

Certain types of incident have to be recorded to meet the requirements of applicable legislation and as such do not need consent. Where consent is needed our internal procedures dictate how and when to obtain it.

As we are connected to the NHS N3 system (Patient records and encrypted email) we are compliant with the Data Security and Protection Toolkit which is re-accredited on an annual basis and dictates our standards of Data Protection. This is fully compliant with the requirements of the Data Protection Act.

For the purpose of the Vantage database the Data Processor is Vantage Technologies. The data is cloud hosted using industry standard technology. There is nothing novel or higher risk about the hosting arrangements.

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?

Our aim is to improve our methods of data recording so that we can offer a better service to our patients and staff. We will not be collecting much more information than is already included in our semi-manual systems. The difference is how we will be able to interrogate the data to ensure we are spotting patterns in accidents/incidents faster and more reliably than we can at present and as a result be able to respond more effectively around patient care and safety as well as wider within our organization.

Our recording of information relating to premises management is also not going to greatly increase in scope but will become much more useful when planning things like scheduled maintenance which will ensure we keep our facilities safe and compliant without having to rely on manual processes.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Given the nature of the information we want to capture in the database we have involved the Clinical Governance and Quality Lead, The Premises Manager and the Support Services Committee (a Board sub-committee). The Quality Lead and Premises manager are leading the implementation project.

Our processors act as a hosting and software development partner and have facilitated the formation of a hospice group to enable the sharing of expertise (but not data).

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

We will gather and process only that data which is required for compliance and the safe and effective operation of the hospice. This is the most appropriate means of achieving our aims that we could identify and has been successfully implemented by our peers in the hospice movement

Information supplied to individuals will be fully compliant with NHS Data Safety guidelines which are also compliant with the Data Protection Act.

Our processors have internal controls and will sign a confidentiality agreement during the course of implementation and before real data is entered.

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**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Inappropriate access to data by Vantage staff	Possible	Minimal	Low
Inappropriate access to data by St Andrews staff	Possible	Minimal	Low
Loss of data from equipment failure	Possible	Significant	Medium
Loss of data due to data hack	Possible	Significant	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**
		Eliminated reduced accepted	Low medium high	Yes/no
Equipment failure	Vantage software is backed up every 24 hours, and the data is held on a RAID array which ensures that failure of a disk drive will not result in data loss.	Reduced	Low	Yes
Data hack	Vantage's hosting supplier is Rackspace Limited, they have ISO/IEC 27001 certification and are also a PCI DSS Level 1 provider.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
SIRO advice provided:		SIRO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
SIRO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:		The SIRO should also review ongoing compliance with DPIA