DPIA – St Martins Housing Trust Customer Relationship Management in Highwater House

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA 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.

Submitting controller details

Name of controller	St Martins
Subject/title of DPO	Customer Relationship Management in Highwater House
Name of controller contact	Head of Residential Care Services

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.
At St Martins Highwater House we use Nourish together with some paper records as our Customer Relationship Management (CRM) system, to log information about the people we support through our service, plus complaints & feedback, and safeguarding vulnerable adults. We also use it to record information concerning our buildings. This includes information related to health and safety, compliance, audits, contractors (including their insurance details etc) and maintenance. We believe that this DPIA is required because, in the event of a data breach, the data recorded in this system could compromise individuals' health & safety, and leave them vulnerable to identity theft.

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 is provided by the individual receiving care and support, and includes:

- name, dob, next of kin and address, if appropriate.
- information about care and support needs.
- recent history relevant to the care and support which may be required, including offending behaviour, substance misuse, and mental and physical health issues.
- risk information that may include information from a third party, for example probation services for people on licence.
- details of others providing care and support, including drug treatment, GP, and Social Services. (see also our LIA, 'Reasonable Expectations').
- support pathway and future planning needs for care and support
- complaints, including any from the public.
- safeguarding concerns.
- referral information from Local Authority/other agencies.
- information about maintenance jobs on our properties.

On occasions there may be information in a person's recent history which is special category or related to criminal offences.

We record contacts with individuals and the nature of the contacts. We also log information about health and social care related appointments and the outcome of these appointments. All of the above data creates an up-to-date picture of the individual and their care & support needs, which enables St Martins to deliver the appropriate support and ensure consistency of service.

The data is only accessible to St Martins Highwater House team members. However, in circumstances where multi-disciplinary team work is required, access is given under Information Sharing Agreements to workers outside of St Martins who deliver care & support to individuals in the support of St Martins.

The data is also available to Nourish Care Systems Limited (NCSL), as they support our Nourish system. The NCSL team is trained in data protection and is contractually obliged to handle sensitive information securely.

Data is stored in a cloud based facility based in London on the Amazon Web Services (AWS). AWS is certified to international security standards ISO9001:2008 (which ensures it has an auditable quality management system in place), ISO27001 (which ensures it actively monitors and reacts to security risks), and SSAE16/ISAE 3402 (which means it is audited by independent third parties). No information will

be transferred by Nourish internationally. All information held by Nourish is hosted in England.

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?

The nature of the data is described above.

We store data related to individuals' health. We also store data related to criminal offences, religion, sexual orientation, racial and ethnic origin if this is considered relevant to the care and support required, and as part of our performance monitoring against protected characteristics which is anonymised for reporting purposes.

Information is logged on Nourish as soon as a person starts to receive care and support from St Martins Highwater House. Information is updated when there has been contact with the person, or new information is provided by the person which is relevant to the provision of care and support.

Property maintenance jobs are recorded as they arise by staff and are linked to the property and the individual who is renting the property from us.

Complaints from all sources are recorded as they arise and are progressed and managed within the system. They are also linked with the individual if named in the complaint.

Safeguarding concerns are recorded as they arise and are linked to the individual.to whom we are providing care and support.

Data covers clients and services in the Greater Norwich area. Clients number approximately 22 at any one time, and approximately35 per year.

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)?
St Martins Highwater House relationship with the individual is care-provider/cared-for in nature. When individuals begin to receive care & support from St Martins Highwater House they are given information about the data recorded including how it will be used, who it will be shared with, the systems used, and who can access the systems. Posters explaining the need for GDPR are on display in all St Martins premises provided for service users. The people we support have capacity (as defined by the Mental Capacity Act 2005) but the majority are considered vulnerable. Our services are for people over the age of 18. Children are not included. To the best of our knowledge there are no prior concerns, issues of public concern or known security flaws with this type of processing. It is not novel. Nourish is a market leader in this application type. St Martins is accredited to the NHS Data Security and Protection Toolkit (DSPT) at the level 'standards met'. St Martins has Cyber Essentials accreditation, which defends against common threats to cyber security. St Martins has an internal IT Technician (with access to further support from Cube Connection if required) to maintain all computer systems, hardware and software. All St Martins staff have completed Data Security Awareness training. Nourish is a secure platform. Data is stored in a cloud based facility based in London on the Amazon Web Services (AWS). AWS is certified to international security standards ISO9001:2008 (which ensures it has an auditable quality management system in place), ISO27001 (which ensures it actively monitors and reacts to security risks), and SSAE16/ISAE 3402 (which means it is audited by independent third parties). No information will be transferred by Nourish internationally. All information held by Nourish is hosted in England.

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?
The purpose of our processing is to provide the best care and support possible to our service users. It ensures consistency of approach and avoids the need for people to tell and retell their story. The benefits of processing for St Martins Highwater House is having access to relevant and up-to-date information to support the delivery of care and support. More broadly it enables us to evaluate and improve our services allowing us to contribute positively to a reduction in homelessness nationwide.

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?
Nourish has been operational at St Martins Highwater House since May 2022. NCSL provides our Nourish licences. Nourish is a leading service management system, built by NCSL. IT support, provided by an internal IT Technician (and Cube Connection if required), ensures St Martins has the best cyber security at all times. St Martins is accredited to the NHS Data Security and Protection Toolkit (DSPT) at the level 'standards met'. St Martins also has Cyber Essentials accreditation, which defends against common threats to cyber security.

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?
Our lawful basis for processing data is 'legitimate interest' and, within that, our additional condition for processing special category data is 'health or social care'. Processing special category data is necessary to provide the best care and support, tailored to the needs and goals identified for and by the individual, and is conducted under the responsibility of CEO Dr Jan Sheldon who owes a duty of confidentiality under an enactment or rule of law. Using a cloud based CRM system means that records are more accessible and secure. Data quality is regularly sampled and audited by the Director of Care Services. We are building an internal audit programme which will assure data quality across the board. Training is given to all staff to help them create records which are accurate, relevant and evidence-based. With NCSL (who support our system) we can perform reviews of the system, including data stored, to ensure that updates can be made and areas fine-tuned as required. Information about how data is stored and used is given to individuals when service delivery begins. Nourish is a secure platform. Data is stored in a cloud based facility based in London on the Amazon Web Services (AWS). AWS is certified to international security standards ISO9001:2008 (which ensures it has an auditable quality management system in place), ISO27001 (which ensures it actively monitors and reacts to security risks), and SSAE16/ISAE 3402 (which means it is audited by independent third parties). No information will be transferred by Nourish internationally. All information held by Nourish is hosted in England.

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) Care/support workers are distracted/called away from their PCs and leave without locking their screens meaning unauthorized people could access data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
2)Passwords are guessed or shared inappropriately meaning unauthorized people could access data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
3)Data is recorded in an inappropriate manner providing subjective information not factual	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
4)Cyber attack meaning unauthorized people could access data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

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)	Regular training and frequent reminders of the dangers of leaving PC screens unlocked. PC's to be located in areas which are not accessible by the people who use our services	Eliminated reduced accepted	Low medium high	Yes/no
2)	Frequent reminders to select passwords which can't be guessed/words which are unrelated. Reminders not to share passwords.	Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item: v1.0	**Name/position/date**	**Notes**
Measures approved by:	Head of Residential Care Services, 3/5/2022.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Head of Residential Care Services, 3/5/2022	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System Data Coordinator, 3/5/22	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Head of Residential Care Services	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	System Data Coordinator and Senior Management Team.	The DPO should also review ongoing compliance with DPIA