DPIA - St Martins Housing Trust Publicity images

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	Publicity images
Name of controller contact	Head of Communications and Marketing

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 we create, obtain, record and use photographic and video images in our publicity campaigns. These images may feature team members, or people we support, or be copyright-free downloadable from the internet. Most images are captured by members of the Communications and Marketing Team (who are most alert to such opportunities) with additional images captured by other team members and passed to the Communications & Marketing Team. All images are filed in a restricted folder within Microsoft Teams which constitutes our publicity image library. 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?
Images are captured using St Martins team member mobile phone cameras, passed via e-mail to the Communications & Marketing Team (where necessary), or chosen from the internet, and filed by the C&M Team in a restricted folder within Microsoft Teams designated for the purpose. Access to this folder is restricted to C&M Team members and the Director of Operations (Internal). Images are used on all or any of the following: St Martins website, social media, newsletter and printed promotional material. On occasion images may be submitted to the media as part of a press release. Verbal consent is obtained at the point of the photograph being taken, with possible uses clearly stated. No high-risk processing is involved as the images are low in volume. Also, all images are carefully created/chosen so as to convey only the faces and no other identifiable personal data of the subjects. Images are tagged with a photo-credit as appropriate. Images are retained for as long as they might be useful in publicity campaigns. They are deleted from the library and no longer used for publicity if/when the C&M Team become aware that an individual subject has died or withdraws their consent. Microsoft Teams has the inbuilt resilience of a cloud-based system (rather than server-based backup).

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 at section 2 above. No special category data or criminal offence data is included.

Images are created/chosen as opportunities arise or as required for specific publicity campaigns.

Images are deleted when judged to be no longer useful, or when a subject is known to have died, or when consent is withdrawn.

The library stands at approximately 3,800 images as at October 2023.

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' relationship with data subjects is either charity/supporter in nature or service/client. Subjects verbally consent to their image being used for publicity purposes. Data subjects entrust us with this personal data. Loss of control might be possible in the event of a data breach which is why we mitigate the risks (steps 4 and 5 below). People from vulnerable groups may be among supporters at any time, but St Martins does not record this information. People from vulnerable groups may be among clients at any time. This type of processing is well established in the charity/supporter and service/client arena and is not novel. St Martins is accredited to the NHS Data Security and Protection Toolkit (DSPT) at the level 'standards met', and is accredited to Cyber Essentials 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.

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 assemble and manage a library of photographic images which are useful in our publicity campaigns.

The intended effect on data subjects is that they will feel valued and involved in furthering the work of St Martins.

The benefit is that St Martins publicity campaigns are successful.

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?

Consultation with stakeholders during the project included St Martins trustees, directors, and HR and Reception staff.

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 is 'consent'. The verbal consent of each data subject is obtained before their image is recorded for use. Our processing achieves its purpose, as evidenced by successful publicity campaigns. No international transfers of data are made.

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) Staff are distracted/called away from their computers without locking them, meaning unauthorized people could access data.	Remote, [✓ possible] or probable	[✓ Minimal], significant or severe	[✓ Low], medium or high
2) Passwords are guessed or shared meaning unauthorized people could access data.	Remote, [✓ possible] or probable	Minimal, [✓ significant] or severe	Low, [✓ medium] or high
3) Information is recorded inappropriately generating inaccurate data.	[✓ Remote], possible or probable	[✓ Minimal], significant or severe	[✓ Low], medium or high
4) Cyber attack allowing access by unauthorized people.	[✓ Remote], possible or probable	Minimal, significant or [✓ severe]	Low, [✓ medium] or high
5) Images taken by St Martins and shared in the public domain could be copied and redistributed without the consent of the data subjects and outside of the context of the original intention	[✓ 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**
2)	Frequent reminders to use passwords which are unrelated, cannot be guessed and not to be shared.	Eliminated **reduced** accepted	**Low** medium high	**Yes**/no
4)	Continued commitment to maintaining Cyber Essentials accreditation.	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 Comms & Marketing 10/10/2023.	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Head of Comms & Marketing, 10/10/2023.	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System/Data Coordinator, 10/10/2023.	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 Comms & Marketing	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