DPIA – St Martins
Closed Circuit Television (CCTV)

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	System Data Coordinator
Name of controller contact	St Martins service managers.

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 selected St Martins premises we use a video recorder with up to 16 cameras as our Closed Circuit Television (CCTV) system, to see and record moving images of people entering the building and at various points inside the building. Additionally, door control/access systems comprise door cameras which may not record images. Where the CCTV systems are connected to the St Martins computer network, recorded image data is accessed via St Martins laptops and smart phones. Each CCTV installation is either located in a secure office with a controlled electronic door entry system for authorised personnel only, or supervised by authorised personnel when in use and locked when unattended. CCTV systems are an important part of security provisions at St Martins, designed to protect those using our buildings. All staff are aware of the CCTV policy and procedures. All users of the buildings are made aware of CCTV usage by signage at the entrance. 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 collected automatically, some systems running 24/7 and others upon motion trigger or other smart event, e.g. line crossing or intrusion detection. Data is stored on hard disk storage devices. The data is only accessible by St Martins team members and the System Administrator. St Martins appoints a System Administrator for each installation (to manage new users & leavers, and provide help to staff if required). Data may be required by St Martins managers or by the Police for use as evidence in the event of a security incident. Data may be shared after satisfactory submission and approval of a release request. No processing has been identified 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?
The nature of the data is described above. It does not include special category data or criminal offence data. Note: St Martins CCTV systems are not of a sophisticated variety which can collect biometric data (e.g. facial recognition or similar) and would bring additional responsibilities and be categorised as 'special category' data. Data is stored on the systems' storage device (hard disk) and kept for up to 90 days before deletion. The systems are on 24 hours a day, 7 days a week. Data is collected according to the system's configuration, either 24/7 or upon motion trigger or other smart event e.g. line crossing or intrusion detection. Data subjects include St Martins staff, users of our services, and visitors to the building. The geographical areas covered are the entrances to buildings and various points within the buildings.

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 the individual is mainly service user/service provider in nature, plus additional visitors to the building. Signage at the entrance make building users aware that CCTV is in use. CCTV use is not unexpected in premises providing services such as ours. Most of the people we support have capacity (as defined by the Mental Capacity Act 2005) but the majority would be 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. 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.

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?
St Martins uses CCTV to provide a safe and secure environment for people who use services, staff and visitors, to prevent the loss or damage to property and assets, and for the prevention, investigation and reduction of crime, which may include the provision of evidential data to the Police and other agencies. The benefit of processing for St Martins is having access to a proven tool which contributes to the provision of security and a secure environment to our service users. More broadly it supports the continuity of 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?
It is accepted practice that CCTV systems are used to help provide a secure environment for our service users, visitors and staff. All staff are aware of our CCTV policy and procedure. All users of the building are made aware of CCTV usage by signage at building entrances. Use of a CCTV system is very well established in St Martins and fully understood by staff operating it. There is no need for further consultation at this stage. 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'. The processing achieves its purpose of providing a secure environment for staff and service users by providing evidence in the case of a security incident. Training is given to all staff who manage CCTV data. Data is stored on the systems' hard disk storage device for up to 90 days. All staff are aware of our CCTV policy and procedure. All users of the building are made aware of CCTV usage by signage at the entrance to the buildings. Individual's rights to their data being protected are supported by our system security measures, including system access being limited to the minimum number of staff.

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 devices 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) Cyber-attack meaning unauthorized people could access data.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
4) CCTV rooms are left unsecured 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 device screens unlocked. Laptops to be located and kept in areas which are not accessible by the people who use our services. Smart phones never left open and unattended.	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:	Service Managers, 12/6/2023	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Service Managers, 12/6/2023	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System/Data Coordinator, 12/6/2023	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:	Service Managers, 12/6/2023	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Service Managers	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	System/Data Coordinator and Service Managers	The DPO should also review ongoing compliance with DPIA