DPIA – St Martins Housing Trust e-mail

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 /DPO (delete as appropriate)	Director of Operations (Internal)

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.
St Martins uses MS 365 and MS Exchange in an hybrid environment as the e-mail system for all staff and some volunteers. We use e-mail to send and receive messages both internally within St Martins, and externally with contacts outside of St Martins. 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?

The e-mail system is used by all St Martins staff and some volunteers and all data is stored in the UK. Backups are encrypted for security. Transmission of email data is end-to-end-encrypted (E2EE).

All users observe the guidelines explained in St Martins policies ‘Privacy’, ‘Data Protection’ and ‘Information Governance’.

An e-mail account and unique e-mail address for each user is created by the system administrator upon request by the user’s line manager. Users are then able to receive and send e-mails using their account and address. If desired, users can create folders within their inbox, for example, to manage different projects.

E-mail data is shared with contacts, both internal and external to St Martins.

All users observe the requirement that no personal data which might constitute a high risk is processed using the e-mail system. This includes outgoing and incoming e-mail messages.

The source of the data (e-mail messages) is both outgoing and incoming messages.

E-mails are sent, replied to and forwarded, and users observe the guidelines explained in St Martins policies (above).

As required by St Martins policies (above), no high risk processing is undertaken.

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 data is e-mail addresses and e-mail messages sent and received.

No special category or criminal offence data is included as users observe St Martins policies (above).

Being a prime communication tool, e-mails are created and saved on a daily basis.

Users manage their e-mail accounts using the available Outlook tools to keep those stored to a minimum.

E-mail messages are mostly exchanged internally with a lesser amount externally nationwide.

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)?

Our relationship with the individuals is user/user in nature.

St Martins users have control over how the data is processed, kept and deleted, but external users too should manage data they send observing data protection guidelines.

All users would expect us to process their data in a responsible fashion, as publicized by our Privacy Notice.

E-mail messages are infrequently used by the people we support, who are often vulnerable but do not include children.

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. Microsoft 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.

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 support the provision of the best care and support possible to our service users. It is an efficient and effective way to share information quickly.

The benefits of processing for St Martins is having access to relevant and up-to-date information to support the delivery of care and support.

More broadly it supports 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?

Microsoft e-mail has been operational at St Martins since 2001

IT support, provided by an internal IT Technician (and Cube Connection if required), ensures St Martins has the best cyber security at all times.

The internal IT Technician acts as system administrator and works continuously to ensure the e-mail platform is fit for purpose.

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'.

Using e-mail in this way supports us in providing the best care and support to our service users. It is an efficient and effective way to share information quickly. We prevent function creep by training our users to manage e-mail records following data protection principles.

Guidance and training is given to all St Martins e-mail users to help them create and manage e-mail records which follow data protection principles.

The internal IT Technician, as system administrator, performs reviews of the system, including data stored, to ensure that updates can be made and areas fine-tuned as required.

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) Inappropriate data is recorded and shared.	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
3)	User training in, and familiarity with, data protection principles and St Martins policies.	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:	Director Operations (Internal), 26/6/2023	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Director Operations (Internal), 26/6/2023	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	System Data Coordinator, 26/6/2023	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Director Operations (Internal), 26/6/2023	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