STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**TRE Project Privacy Impact Assessment**
Effective Date:	**07 Jun 2019**
Reference Number:	**SOP-07-01**
Version Number:	**1.3**
Owner:	**Information Security Manager,**
Review Date:	**03 Nov 2019**

Table of Contents

1. Purpose

It is strongly recommended that a Privacy Impact Assessment (PIA) document be completed for each TRE project. This should begin as early on in the project as possible and be revisited as the project develops. It is a legal requirement of any high risk project. This document provides sections that should be completed, with guidance on their completion in grey italics.

The TRE, and all systems contained within, is involved in handling information that must be managed in a way that ensures its confidentiality, availability and integrity. Implementing security controls throughout the lifecycle of a system can help the TRE achieve its ISMS objectives, regulatory requirements and the needs of its users.

2. Scope

This document can be used for any that have not already done a PIA. Other PIA templates may be acceptable for TRE projects; Greater Manchester Connected Health City projects, for example, have their own template. Contact the Information Governance Manager to check whether you can use another template besides this one.

3. Responsibilities

The PIA can be completed by any relevant project member. It is expected that other project members and, where applicable, external stakeholders be consulted with during the PIA process.

Contact the Information Governance Manager and for guidance on completing a PIA.

The Information Security Manager should be informed of any matters that are high risk.

4. Procedure

4.1. About this PIA

A PIA is a process which helps organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy when designing and implementing a new project. An effective PIA will allow organisations to identify and fix problems at an early stage when addressing them will often be simpler and less costly. Conducting a PIA involves working with personnel from within the organisation, with partner organisations and with the people affected by the project to identify and reduce privacy risks.

The Information Commissioner's Office has set out the main steps of a PIA (summarised on page 11 of the ICO's PIA Code of Practice):

- Identify the need for this PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

The headings in this document follow this order.

Of particular importance to this PIA is the step of consulting internal and external stakeholders. As the code of practice explains, consultation enables an organisation to understand the concerns of those affected by the project; improves transparency by making people aware of how information about them is being used; and provides an organisation with the opportunity to benefit from wider views and from expertise that may not exist within the organisation itself. You should list all those consulted during the PIA process in the
Consultation process section.

4.2. Identify the need for this PIA

4.2.1. Project Overview

What does the project involve
Who is leading on the project?
What other information has been published about the project or its stakeholders?

4.2.2. Why a PIA is needed

Include details of any privacy issues relevant to the project including:

Table 1 Informed consent[1]. The more answers of 'no' the less autonomy the subjects have and the more sensitive the situation in terms of re-use.

1. Are the data subjects aware that their data have been collected in the first place?	Yes / No
2. Have the data subjects consented to the collection of their data?	Yes / No
3. Were the data subjects completely free to give consent to the collection of their data or have they agreed to collection because they want something (a good or service) and are required to hand over some data in order to obtain it?	Yes / No
4. Are the data subjects aware of the original use of their data?	Yes / No
5. Have the data subjects consented to the original use of their data?	Yes / No
6. Have the data subjects consented in general to the sharing of an anonymised version of their data?	Yes / No
7. Are the data subjects aware of the specific organisations that you are sharing their anonymised data with?	Yes / No
8. Have they consented to your sharing their data with those organisations?	Yes / No
9. Are the data subjects aware of the particular use to which their anonymised data are being put?	Yes / No
10. Have they consented to those uses? [2]	Yes / No *See comment in 6 above*

[1] These questions come from the Anonymisation Decision Making Framework (2016), with minor rewording.

[2] For Q7-10 of Table 1 UoM is the receiving organisation, and the questions are considered in terms of the sensitivity of data we are requesting.

Table 2 Expectations of data subjects. The more answers of ‘yes’, the more sensitive your data situation.

1. Do you (the sending organisation) have a relationship with the data subjects?	Yes / No
2. Does the receiving organisation have a relationship with the data subjects?	Yes / No
3. Do you and the receiving organisation work in different sectors?	Yes / No
4. Is your organisation’s area of work one where trust is operationally important (e.g. health or education)?	Yes / No
5. Is there an actual or likely perceived imbalance of benefit arising from the proposed share or release?	Yes / No

Table 3 Nature of the data. The more answers of ‘yes’, the more sensitive your data situation.

1. Are some of the variables sensitive?	Yes / No
2. Are the data about a vulnerable population?	Yes / No
3. Are the data about a sensitive topic?	Yes / No

4.3. The information flows

Details of data being shared and who and where to/from
Consider including a list of data items as an Appendix
A diagram with boxes and arrows can be a really helpful illustration here

Figure 1 Data flow diagram

4.4. Identify the privacy and related risks

Table 4 Issues of privacy and associated risks to individuals, legal obligations, and the University of Manchester (the legal entity that hosts the TRE).

Include all issues (or potential issues) that you have identified.
Add rows or refer to other risk assessments as required. For long tables it makes sense to order or group them as appropriate.

Privacy issue	Risk to individuals	Compliance risk	Organisational risk
	e.g. distress, loss of privacy, sense of intrusion	*e.g. Data Protection Act, General Data Protection Regulations, Human Rights Act, Common Law Duty of Confidentiality*	*e.g. civil action, fines, loss of reputation, media furore*

4.5. Identify privacy solutions

Table 5 Management solutions to the risks identified in Table 4, with evaluation of how much the risk has been reduced. Risks are evaluated as to whether implementing each solution brings a justified, compliant and proportionate response given the final impact on individual privacy and the project's aims. Issues that remain high risk should be reported to the ISM for inclusion on the TRE Risk Register.

Risk	Solutions to reduce risk	Evaluation
Risk identified in Table 1	*e.g. don't share certain data, collapse or mask rare values, staff training, hide certain variables from TRE users, produce summary statistic then delete sensitive input variables* *Refer to TRE SOPs if relevant*	

4.6. Risks and actions identified in the PIA

Table 6 Actions agreed for reasonable approach to each risk, with details of responsible project members.

Risk	Action to be taken	Date for completion of actions	Responsibility for action
	e.g. revise the requested dataset	*Before data transfer date*	

4.7. Consultation process

List people and meetings that informed this PIA

4.7.1. Contact for future privacy concerns

Insert name, affiliation, and email address here

4.8. Supporting information

Include or link to additional information like a data specification
If you are managing personal data you need to maintain a Record of Processing, including the legal basis and other details listed in GDPR Article 30.

5. Cross-referenced ISMS Documents

Number	Type	Title
<NO DATA>	<NO DATA>	<NO DATA>

6. Appendices

6.1. Further reading & guidance

Anonymisation Decision Making Framework (2016) http://ukanon.net/ukan-resources/ukan-decision-making-framework/
European Guidelines on Data Protection Impact Assessment (2017):
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
European Data Protection Board opinion on Data Protection Impact Assessments (2018)
https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf
ICO's PIA Code of Practice Editable Annexes (2014): https://ico.org.uk/media/1042836/pia-code-of-practice-editable-annexes.docx
ICO Data Protection Impact Assessment webpage including checklists (2019): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/