THE UNIVERSITY of EDINBURGH

Assessment Details

Name Example Assessment

Respondent Ailsa Niven

Date Completed 09/09/2021 09:46

Approver Rena Gertz

Stage Completed

Result Approved

Assessment Questions

1 Overview

1.1 **Research Outline**

Summarise what the research 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. Explain why and how the processing of information is necessary to that work?

Response

In this study, researchers aim to understand how young children in refugee families interact with digital technologies in their home environments, in order to adapt to the Scottish culture. The researchers are interested in adopting an approach that would not interfere with the participants' routines, and through consultation with the research participants it became clear that families were familiar with WhatsApp for daily communication, and this would be their preferred and most easily accessible mode of communication.

In order to elicit information on children's interactions with technologies the researchers will use a method called 'living journals' (Savadova & Plowman, 2020). The living journals entail that the parents document via WhatsApp the children's daily activities for a brief period of time by taking pictures of the children, making videos of their interactions; they can also provide textual and voice explanations to the researchers about the children's activities on WhatsApp. Thus, adults can become proxy researchers, collecting data about their children in their own time, and in a context that is familiar and convenient for themselves and the children.

Parents will send the information via WhatsApp to the researchers who will receive the information on their own personal password-protected devices, and through the desktop version on University password-protected devices. Due to the unavailability of a university registered mobile phone, the researchers will use their own personal phone numbers to enrol on the WhatsApp group. (Rena - it is possible to set up an account specific for the project - that would require a university mobile phone number - should we detail that?)

The researchers will upload the data from WhatsApp to secure university space (datastore) for storing, analysis and reporting. Transcripts of the recordings will be created but all participants will be de-identified in these transcripts. The transcripts will also be stored in secure university space.

1.2 **Describe the information flow**

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows – where you are getting the data from, where it will be stored and where it could be transferred to. You should also say how many individuals are likely to be affected by the project.

e.g. Data will be collected from research participants via online forms

↓

Data will be stored encrypted on departmental drives

↓

Pseudonymised dataset will be provided to Department X along with report

Response

COLLECTION - Participants' names and phone numbers will be collected initially by the researchers to enable the set up of the WhatsApp group. Participants will previously have shared their personal details with WhatsApp in order to make use of the app.

Research data will be collected from participants via WhatsApp following informed written consent from the parents, and verbal consent from the children. Parents will record via WhatsApp the children's daily activities for a brief period of time by taking pictures of the children, making videos of their interactions; they can also provide textual and voice explanations to the researchers about the children's activities on WhatsApp.

STORAGE - The participants' names and phone numbers will be stored separately from the research data on DataStore. Parents will send research data via WhatsApp messages to the researchers and will be accessed via a password protected personal devices, and using WhatsApp PC on a University device to transfer the data to a safe online repository hosted by the University (DataStore). The data will be stored for two years after the end of the study, when it will be destroyed.

REPORTING - On dissemination of the findings, all data will be anonymised. Pictures of the children, which may show their faces and which may be considered identifiable, will be anonymised (via blurring) unless parents have explicitly consented to their use.

2 Compliance with Privacy Laws

2.1 **Check**

Data Protection legislation is relevant to any DPIA, and this section forms the data protection compliance check which should always be carried out. The Data Protection Officer will be able to advise you on the relevance of other privacy laws.

2.2 **What type of personal data are you processing?**

*For guidance on what personal data is, consult the**definitions.***

Response

Any other personal data

Justification

None

2.5 **List the personal data you are going to process?**

*For guidance on what personal data is, consult the**definitions.***

Response

Initial information collected for participation in the study will include for Parents: Full Name, Email address, Phone Number. This information will be collected at the same time as the participant consent.

The research data could include videos and photos with images and voice recordings that are potentially identifiable, so this information is also classed as personal data.

2.6 **Which of the legal bases in Article 6 (1) will provide a lawful basis for the processing?**

For research the legal basis will typically be task carried out in the public interest or 'public task'.

*Consult the document **Guidance – how to determine the legal basis for processing personal data** for information on the other potential legal bases.*

Response

Public Tasks

Justification

For research the legal basis will typically be task carried out in the public interest or 'public task'.

2.7 **Special Categories of Personal Data**

*If special categories of personal data are going to be processed, which of the legal bases in Article 9 (in addition to the Article 6(1) legal bases) will provide a legitimate basis for that processing? Consult the **special category guidance** for information on determining the legal basis for special category data.*

For research the legal basis for special category personal data will typically be Article 9 (2) (j) – necessary for research in the public interest or 'archive, statistical and research purposes'.

Note – special categories of personal data are personal data consisting of information as to (a) the racial or ethnic origin of the data subject, (b) political opinions, (c) religious beliefs, (d) Trade Union membership, (e) physical or mental health, (f) sexual life, (g) genetic data and (h) biometric information.

Response

Not Applicable

Justification

None

2.8 **How are individuals being made aware of how their personal data will be used?**

How are individuals being made aware of how their personal data will be used? If you supply participants with a Participant Information Sheet (PIS), please attach the PIS.

*There is a template PIS available within the**Research and the General Data Protection Regulation** guidance.*

Response

Information regarding use and management of personal data is included in the participant information sheet and a link to WhatsApp privacy policy will be in included when inviting the participants to the study:
https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en

This is further explained when discussing with the participants to provide an introduction to the study. (NEED EXAMPLE PIS TO UPLOAD)

2.9 **Does the activity involve the use of existing personal data for new purposes?**

Response

No

Justification

None

2.10 **Is there a way to check that the data collection procedures are adequate, relevant and not excessive in relation to the purpose for which the data will be processed?**

Response

The research study has been designed so that only minimal data to meet the study aims are collected

2.11 **How will the personal data be checked for accuracy?**

Response

The participants will provide the researchers with their names and telephone numbers, and the researchers will confirm with the

participants that these are accurate so that they can communicate directly with the participants.

The videos and images will be sent directly from the research participants, so there is no need to confirm accuracy.

2.12 **Will there be set retention periods in place in relation to the storage of the personal data?**

Will there be set retention periods in place in relation to the storage of the personal data? If 'Yes', you will need to include details of this in your PIS.

If you applying the research exemption that the data in intended for future use, you can select 'No'.

Response

Yes

Justification

None

2.13 **What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?**

Response

Names, email addresses and phone numbers will be stored on the university's secure server datastore, separately from the research data. .

In terms of sharing of research data, the participants will access the social media platform via their own personal devices, and will be advised to ensure these are password-protected.

Data are protected from interception through end-to-end encryption. From WhatsApp: “End-to-end encryption means that your messages are encrypted to protect against us and third parties from reading them.”

Once received by the research team, the research data will be accessed via WhatsApp pc and uploaded to secure datastore, and will only be accessed by the research team. From the recordings, transcripts will be created.

The whatsapp conversation will be deleted at the end of the data collection period.

2.14 **Has the personal data been evaluated to determine whether its processing could cause unwarranted damage or distress to data subjects?**

Response

Yes

Justification

There is no anticipated risk

2.15 **Do you use a data processor?**

Response

No

Justification

None

2.17 **Will you share the data with an external third party?**

Response

No

Justification

Whatsapp as the provider of the app will transfer the data. However, the content of the data are protected from interception through end-to-end encryption. From WhatsApp: “End-to-end encryption means that your messages are encrypted to protect against us and third parties from reading them." Whatsapp do not retain the messages in the ordinary course of service - instead messages are stored on the individual device, and not a whatsapp server. Once messages are delivered they are deleted from the server (if delay in delivery they are stored encrypted for up to 30 days).

Whatsapp do collect user data (e.g., location, usage data etc) but this is not specific to the research project. Participants will have independently agreed to using whatsapp and its terms and conditions.

2.19 **Will you be transferring personal data to a country outside of the European Union or the European Economic Area (EEA)?**

Countries in the EU
Countries in the EEA

Response

No

Justification

None

2.23 **If the data will be anonymised, is it likely that a ‘motivated intruder’ will be interested in attempting re-identification by linking the data with other information available to them?**

*For guidance on 'motivated intruders', please see**here.***

Response

No

Justification
None

2.24 **From the Data Protection compliance check in this section we have concluded:**
Have you satisfied all the requirements asked for above? If you answer no, then please give a reasoning why and why you believe the DPIA should still be approved.

Response
We have concluded that if the research project goes ahead as detailed here, it is data protection compliant.

Justification
None

3 Screening

3.1 **Screening**
Answer the following questions to determine any potential privacy risks in your research.

You will then be asked to explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted about potential risks (members of your research team, supervisor, research sponsor...)?

3.2 **Will the research involve the collection of new identifiable or potentially identifiable information about individuals?**

Response
Yes

Justification
Participants will share videos and images of family activities

3.3 **Will the research compel individuals to provide information about themselves, i.e. where they will have little awareness or choice?**

Response
No

Justification
Participants will be fully informed as to the requirements of the study. More specifically, they are asked to share pictures or videos that depict their children's routine interactions with artifacts and people in the home, when prompted by the researchers' questions, for the stated given period of time. The adults' consent is obtained in writing for these purposes, whereas verbal consent is sought from the children as well as assent is maintained. The parents choose whether they agree to send such visual materials to the researchers or to provide text or audio descriptions of their children's interactions instead. The parents also choose how and whether these visual materials can be used in publications, and whether these should be anonymised (e.g. by blurring the children's faces in pictures).

3.4 **Will identifiable information about individuals be shared with other organisations or people who have not previously had routine access to the information?**

Response
No

Justification
Participants will already have signed up to WhatsApp prior to participation in the study, and will have agreed to their specific terms and conditions.

In terms of the research data, we this is not shared with WhatsApp as they state:

"we will always protect your personal conversations with end-to-end encryption, so that neither WhatsApp nor Facebook can see these private messages. We don't keep logs of who everyone's messaging or calling and can't see your shared location so we cannot and do not share this with Facebook. We need your contacts to provide the service, but don't share your contacts with Facebook".

3.5 **Are you using information about individuals for a purpose it is not currently used for or in a new way, i.e. using data collected to provide care for an evaluation of service development?**

Response
Yes

Justification
The data will be used for a research study

3.6 **Will there be new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?**

Response
No

Justification
None

3.7 **Where information about individuals is being used, would this be likely to raise privacy concerns or expectations, i.e. will it include health records, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress?**

Response

No

Justification

None

3.8 **Will the project require you to contact individuals in ways which they may find intrusive, i.e. telephoning or emailing them without their prior consent?**

Response

No

Justification

None

3.9 **Will the project result in you making decisions in ways which can have a significant impact on individuals, i.e. will it affect the care a person receives?**

Response

No

Justification

None

3.10 **Does the project involve you using new technology which might be perceived as being privacy intrusive, i.e. using biometrics, facial recognition or automated decision making?**

Response

No

Justification

None

3.11 **Is a service being transferred to a new supplier (re-contracted) and the end of an existing contract?**

Response

No

Justification

None

3.12 **Is processing of identifiable/potentially identifiable data being moved to a new organisation (but with same staff and processes)?**

Response

No

Justification

None

3.13 **Consultation to address privacy risks**

Explain what practical steps you will take to ensure that you identify and address privacy risks highlighted in the preceding questions. Who should be consulted about potential risks (members of your research team, supervisor, research sponsor...)?

Response

TO ADD

4 Risk identification

4.1 **Risk identification and assessment**

Together with the other stakeholders, now list all the risks you can identify. Below, you will find a list of common risks. If any of these apply, choose them by answering 'yes' and providing a short description of the risk and how you would mitigate the risk.

If the risk applies – select 'Yes'. As a result you will be require to:

1. Provide a brief explanation / consequence of the risk occurring
2. Provide a brief explanation of the mitigating factors that will be undertaken to either eliminate or lower the risk
3. In considering the defined mitigation measures, determine the likelihood of the risk occurring to be Low, Medium or High
4. In considering the defined mitigation measures, determine the impact on the data subjects and on the University to be Low, Medium or High

If the risk does not apply, select 'No'

4.2 **Possibility that information is shared inappropriately.**

4.2 **Possibility that information is shared inappropriately.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
NA

4.5 **Personal data may be used for a new and different purpose without the knowledge of the data subjects, perhaps due to a change in the context in which the data is used.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
None

4.8 **New surveillance methods such as CCTV, email monitoring etc. may be an unjustified intrusion on people's privacy.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
None

4.11 **Actions taken against individuals as a result of collecting information about them might be to their detrment or cause damage/distress.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
None

4.14 **People cannot participate in research anonymously because participants may become identifiable again due to data linkage, low participant numbers, geographical location, transfer of data, or access of data.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
Yes

Justification
Participants may share data that are identifiable (e.g., images) - but these will only be used in dissemination materials without anonymisation procedures if the parent explicitly consents.

4.15 **What can you do to eliminate or at least reduce the risk?**
Explain all mitigation measures you will put in place.

Response
Participants will be fully aware of the options, and will provide explicit consent for use of potentially identifiable research data

4.16 **Is the likelihood of the risk manifesting after the mitigation measures low, medium or high? Provide an explanation for your choice.**

Response
Low

Justification
We anticipate that participants would only consent to use of identifiable images if they perceive the risk as low

4.17 **Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information if anonymity is what people were led to expect.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
No

Justification
None

4.20 **Collecting information, matching and linking identifiers or whole datasets might mean that data are no longer anonymous if anonymity is what people were led to expect.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
(No)

Justification
None

4.23 **Excess information collection or information not properly managed can lead to creation of duplicate records.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
(No)

Justification
None

4.26 **If a retention period is not established information might be used for longer than necessary.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
(No)

Justification
A clear retention period has been specified (two years post project completion)

4.29 **The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the University.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
(No)

Justification
None

4.32 **Public distrust about how information is used can damage the University's reputation and lead to less willingness to participate.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
(No)

Justification
None

4.35 **Data loss causing damage or distress to individuals or damage the University's business.**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
(No)

Justification
None

4.38 **Despite proper security, is there an increased possibility of external unlawful access to the data such as hacking?**
If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response
(No)

Justification

None

4.41 **Using an external data processor or sharing with another data controller increases the risk of unlawful access to personal data.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

Yes

Justification

Using WhatsApp ?

4.42 **What can you do to eliminate or at least reduce the risk?**

Explain all mitigation measures you will put in place.

Response

We have done due diligence in using WhatsApp and know that the messages are encrypted end to end and are not access by WhatsApp

4.43 **Is the overall residual risk after the mitigation measures low, medium or high? Provide an explanation for your choice.**

Response

Low

Justification

None

4.44 **Are you transferring personal data to a non-EEA country using Standard Contractual Clauses as a safeguard?**

Since the European Court of Justice decision in July 2020, a special risk assessment is required for transfer of personal data in particular to the US but also to other non-EEA countries. Please assess how likely it is that despite the use of the Standard Contractual Clauses the data is likely to be accessed, for example under the Patriot Act in the US.

If the answer to this question is 'yes', then this question will be approved by your Head of School.

Response

No

Justification

Or do we say yes here if using WhatsApp?

4.47 **Any other risk you have identified - describe below.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

None

4.50 **Any other risk you have identified - describe below.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

None

4.53 **Any other risk you have identified - describe below.**

If this risk applies, click 'yes' and give a brief explanation of why the risk applies.

If the risk does not apply, click 'no'

Response

No

Justification

None

6 Submit

6.1 **Submit**

Please now click the blue 'Submit' button in the bottom right corner.