Privacy Impact Assessment

Covid Vaccination Centre Volunteers

OFFICIAL WMFS- LOW
Ownership: [Martin Ward-White]
Date Issued: [22/01/2021]
Version: [1] Status: [TBC]

Revision and Signoff Sheet

Change Record

Date	Author	Version	Comments

Approval

Name	Version	Approved	Position	Organisation	Date

Distribution

Name	Position	Organisation

Document Properties

Item	**Details**
Document Title	**Privacy Impact Assessment**
Author	**Martin Ward-White**
Creation Date	**22/01/2021**
Last Updated	

OFFICIAL WMFS – LOW

Contents

Contents

OFFICIAL WMFS – LOW

1. Privacy Impact Assessments

It is West Midlands Fire and Rescue Service (WMFRS) policy to follow best practice and use Privacy Impact Assessments (PIA) for relevant activities in order to identify and manage any privacy impact risks. This will support compliance with the requirements of the Data Protection Act 1998 (DPA) and Human Rights Act 1998.

Failure to recognise and mitigate adverse privacy impacts could result in reputational damage and possible enforcement action against WMFRS

These questions are intended to help you decide whether a PIA is necessary. Answering 'Yes' to any of these questions is an indication that a PIA must be completed. If this is the case, proceed to Section 2.

Screening Questions	**Yes/No**
Will the project involve the collection of new information about individuals?	**YES**
Will the project compel individuals to provide information about them?	**YES**
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**YES**
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**YES**
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	**NO**
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	**YES**
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	**YES**
Will the project require you to contact individuals in ways that they may find intrusive?	**NO**

2. Privacy Impact Assessment

You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA.

2.1 Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project.

Also summarise why the need for a PIA was identified (this can be drawn from your answers to the screening questions).

WMFS has entered into a partnership with St Johns Ambulance which will see WMFS employees support the national Covid vaccination effort through providing a number of volunteering roles:

- **Vaccinator**
- **Patient Advocate**
- **Patient Carer**

St John Ambulance require WMFS volunteers to have an enhanced DBS check which will be undertaken by St John Ambulance. As part of this process, St John Ambulance are required to collect and verify identification documents for each volunteer. In order to achieve this in the most efficient way possible, WMFS employees will hold virtual appointments with volunteers to validate and record information such as names, identification document numbers (i.e driving licence and passport) and utility bills/ bank statements to certify home addresses. This will be collected by WMFS from employees, with information collated on a secured spreadsheet and sent through to St John Ambulance in order to complete the enhanced DBS process. The requirements for DBS have been set by St John Ambulance who will be the final decision makers as to the suitability of volunteers from WMFS.

The information collected will be that which is a requirement inline with government guidance around DBS: https://www.gov.uk/guidance/documents-the-applicant-must-provide

In addition to information collected for DBS purposes, there is also a requirement for WMFS to collect information around the health of individuals volunteering for the vaccination programme. This form will be collected by WMFS and provided to St Johns ambulance who will make the final decision as to whether a volunteer meets the health requirements for the role.

2.2 Describe the information flows

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. You should also say how many individuals are likely to be affected by the project.

Personal data in relation to volunteers will be provided by the volunteer themselves who, as part of the volunteering process will be required to give consent for the information to be processed and handled by WMFS and St John Ambulance.
Data will be collected through a mixture of and online form through the St John Ambulance Service DBS Portal and a word document form that will be completed by the volunteer and sent to a dedicated email address that is only accessible to WMFS employees who are directly involved in this project so are required to access the information.

As volunteering is open to all employees of WMFS who meet the NHS criteria, it is difficult to establish the final numbers of people who will be involved in this project. As of 21/01/2021 there were 160 volunteers.

Data collected through the St John Ambulance Service portal will be processed and stored by st Johns. Data collected by WMFS on behalf of St John will be collected utilising WMFS systems and stored on WMFS Office 365 servers, before being deleted once both the DBS and Health information has been provided to St John.

2.3 Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

The provision of data and information is voluntary and only required from employees who wish to volunteer for the Covid national vaccination programme. Data and information will be provided directly by the employee via an agreed format and these employees will be notified as to what will happen to the data collected and why it is required. Information about the project is accessible to all WMFS employees via the MESH page.

https://wmfs.sharepoint.com/sites/MeshHub/SitePages/WMFS-Joins-Vaccination-Effort.aspx

Volunteers can withdraw at any time from the project and should this be the case their data will be deleted from both St John systems and WMFS systems.

2.4 Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks.

Annex three can be used to help you identify the DPA related compliance risks.

- **Loss of data through illegal activity.**
- **Not compliant with GDPR legislation.**
- **Unauthorised Access to data.**

2.5 Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

- **Office 365 which is used by both St John Ambulance and WMFS has already been accessed as GDPR compliant.**
- **The infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure data centres.**
- **Network firewalls built into both St John Ambulance and WMFS systems.**
- **The accounts will be password protected, with only authorised personnel having the password.**
- **All personnel accessing the account will have undertaken the GDPR and Management of Information Ecademy Course.**
- **An MOU has been created to ensure that an agreement is in place around the collection and processing of personal information.**
- **St John Ambulance have provided WMFS with their Privacy statement and policy, https://www.sja.org.uk/privacy-policy/**

2.6 Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
As detailed in section 2.4 – Identify the Privacy & Related Risks.	**All of the solutions detailed in Section 2.5 – Identify Privacy Solutions.**	

2.7 Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

TBC

3. Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the Data Protection Act (DPA) or other relevant legislation, for example the Human Rights Act 1998.

3.1 Principle 1 – Lawful, fair and transparent

Personal data shall be processed fairly, lawfully and, in a transparent manner in relation to the individual. To enable this then:

a) at least one of the lawful conditions in Article 6 is met as detailed below, and
b) in the case of sensitive personal data, at least one of the conditions in Article 9 is also met.

- Have you identified the purpose of the project?
- How will you tell individuals about the use of their personal data?
- Do you need to amend your privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act?
- Have you identified the social need and aims of the project?
- Are your actions a proportionate response to the social need?
- If the project involves marketing, have you got a procedure for individuals to opt in for their information being used for that purpose?

3.2 Principle 2 – Purpose Limitation

Personal data shall be obtained only for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data?
- Have you identified potential new purposes as the scope of the project expands?

3.3 Principle 3 – Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed.

- Have I only collected the information that is necessary?
- Is the quality of the information good enough for the purposes it is used?
- Which personal data could you not use, without compromising the needs of the project?

3.4 Principle 4 – Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary?

- How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- What mechanisms have you in place to update/amend the information?

3.5 Principle 5 – Storage Limitation

Personal data shall be kept in a form that permits the identification of data subjects for no longer than necessary for that purpose or those purposes for which the personal data is processed.

- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software that will allow you to delete information in line with your retention periods?

3.6 Principle 6 – Integrity and Confidentiality

Personal information should be processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing, accidental loss or destruction, or damage using appropriate technical and organisational measures.

- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?
- If you will be making transfers, how will you ensure that the data is adequately protected?

3.7 Principle 7 – Accountability

Are you able to show that you comply with the other 6 principles?

4. Legal reasons for processing

In order to ensure that all information is processed lawfully and transparently then one of the following conditions need to be met. Processing will only be lawful if ONE of the following conditions is met:

Is this processing needed for some legally-defined public purpose? Then its condition is **public interest** - Processing of personal information is required to carry out our official functions or a task in the public interest and WMFS has a legal basis for the processing the information under UK law.

Is this required to deliver an agreement with the individual? Then its condition is **Contract** - Processing is necessary to meet contractual obligations entered into by the individual. – contracts are not just for purchasing but can include other activities such as employment activities.

Am I required to do this by law? Then its condition is **Legal Obligation** - Processing is necessary to comply with legal obligations of WMFS. What activities are we legally bound to carry out under Fire and Rescue Services Act and what personal information do we collect as result of these activities

Is this processing truly optional for both the organisation and the individual? Then its condition is **Consent** - Data subject gives consent for one or more specific purposes. – this should not be the first option but consider all other options first

Is this processing needed to protect someone's life? Then its condition is **Vital Interests** - Where processing the information is in a life or death situation.

Is the processing necessary for your legitimate interests or the legitimate interests of a third party? Then its condition is **Legitimate Interests -** This applies where you are using people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to identify a legitimate interest, show that the processing is necessary to achieve it and balance it against the individual's interests, rights and freedoms.

If your project does not fit into any of the above then contact Data Management.