

Data Protection Impact Assessment (DPIA)

Mental Health First Aid

December 2019

Data Protection Impact Assessment (DPIA) – Mental Health First Aid

1. Introduction

The purpose of this document is to report on and assess against any potential Privacy Impacts as a result of the formulation, roll out and ongoing running of the Mental Health First Aid procedure and its network of Mental Health First Aiders.

2. Document metadata

2.1 Name of Project: **Mental Health First Aid**

2.2 Author of report: Scott Watson

2.3 Date of report: 20 September 2019

2.4 Name of Information Asset Owner (IAO) of relevant business unit: **Derek Mackintosh**

2.5 Date for review of DPIA: Initially 6 months then annually (unless any known changes to processing occur)

Review date	Details of update	Completion date	Approval Date
0.1	To mitigate risks with the introduction of Mental Health First Aid	20.09.2019	21.09.2019
0.2	Reviewed for GDPR compliance	23.09.2019	24.09.2019
0.3	Reviewed and legal basis for processing defined by legal counsel	01.10.2019	02.10.2019

3. Description of the project

3.1 Description of the work:

The Scottish Government (SG) strives to create a workplace which promotes wellbeing and supports those who are directly and indirectly affected by mental ill health. This procedure is an organisational approach to ensure mental health first aid support is provided in the workplace as an early intervention.

Staff who seek the support of a Mental Health First Aider (MHFAr) will contact the Occupational Health and Safety branch via telephone or by the Mental Health First Aid Mailbox.

This may resolve their issue or alternatively through conversation it may be appropriate for a MHFAr to make contact with the individual for face to face contact.

Those who volunteer to be a MHFAr will first need to complete an introductory course, this introduces the prospective MHFArs to some of the difficult themes that they may face. Those that feel they can fulfil the role must then complete a 2 day accredited MHFA course to become competent certified workplace Mental Health First Aider.

A corporate database accessible only by the Occupational Health and Safety branch will be maintained to review coverage across the estate, the MHFARs email addresses will be used to communicate with them

Where a MHFAR completes a conversation they will be asked to complete a support conversation log, this is a simple tick box and records no directly identifying data about those seeking assistance. The recording of the MHFARs name will allow the branch to rotate/alternate MHFARs to reduce the pressure on each MHFAR.

MHFARs will not be required to record any details or information and it is understood that the conversations will remain confidential.

3.2 Personal data to be processed.

Variable	Data Source
Mental Health First Aiders workplace email address, location information and contact number. Training information (dates of completion)	Request to join Mental Health First Aid Network and communications. Data already available on staff directory.
Directorate of individual having a support conversation.	Recorded during support conversation between MHFAR and individual seeking support

3.3 Describe how this data will be processed:

The data will be added to a Mental Health First Aider/duty holders corporate database administered by members of the Occupational Health and Safety Branch. The data will be used to communicate with the organisations Mental Health First Aiders for informative mailings and when required to respond to assist an individual.

3.4 Explain the legal basis for the sharing with internal or external partners.

There is currently no legal basis for establishing and maintaining the Mental Health First Aid Network and there will be no data sharing internally or externally other than during internal email distribution to the volunteer Mental Health First Aiders. When UK government obtain royal consent it will become part of our public task to offer any mandatory service legislative powers stipulate.

Meantime, to promote wellbeing, Core SG wish to offer this service as an early intervention. When a member of staff accesses this service the processing of their personal data is lawful under GDPR Article 6 (1) (a) as the data subject has given their consent to his/her personal data being processed by taking up the support service we provide and can withdraw from using the service at any time.

In the event that emergency services support is required whilst a member of staff is using the service, processing of special category data is lawful under GDPR Article 9 (2) (c). This is to protect the vital interests of the data subject or a third party from harm, due to any mental illness or episode which may occur.

The privacy notice will be transparent stating that we are committed to protecting their privacy when they use our services (either via the website, telephone, email or other method of communication) in accordance with EU GDPR. If we ask them to provide certain information by which they can be identified when using our services, it will only be used in accordance with our privacy statement. Please note they retain the right to remain anonymous during their contact with the advice line but we will still retain a record of the contact they have with us.

If personal data is shared with emergency services this is in exceptional circumstances for the preventative and protective measures necessary to protect the general public and to minimise risk to

health. Personal data which is retained will be anonymized data which will be held for statistical and training purposes only.

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
Occupational Health and Safety Branch	Leading on procedures to implement and support the network of MHFARs.
Corporate Health Safety and Wellbeing Committee	Lead body in corporate decisions involving Health and Safety and Wellbeing related matters
Council of Scottish Government Unions	Lead body on matters relating to staff consultation
All Core Directorate staff	Whom the process and the result network of MHFARs will be able to provide assistance.

4.2 Method used to consult with these groups when making the DPIA.

At Corporate Health Safety and Wellbeing Committee meetings which include Senior Managers, Human Resources and Council of Scottish Government Unions.

4.3 Method used to communicate the outcomes of the DPIA.

Inclusion and Health Safety and Wellbeing committee and passed to committee members.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

Where an individual from an Agency, NDPB other body contacts the core support line within a core building the Occupational Health and Safety Branch may be able to offer assistance, but would try to direct to their own organisation depending upon the situation at time of call (experiencing difficulty V crisis).

The training organisation will hold a list of names of course participants to issue certificates to those that complete the Mental Health First Aid Course. It is recommended that this training is refreshed every 2 years. OHSB have a programme in place to cover all training aspects.

5.2 Anonymity and pseudonymity

Only the MHFARs name will be recorded on the conversation log, no other personal or identifying details will be recorded for any other person (i.e the person they had a conversation with).

5.3 Technology

There are no additional technological methods for data processing.

5.4 Identification methods

Only the MHFAR will be identifiable to the Occupational health and Safety Branch. Identifying data about those who sought assistance will not be recorded.

5.5 Sensitive/Special Category personal data

An individual may disclose sensitive data to a MHFAR during conversation but this is only during the conversation and MHFARs have been instructed that this information will not be recorded in any format, only abstracted route cause information.

5.6 Changes to data handling procedures

We are unlikely to change the method of handling the data but if any change a review of this assessment will be required.

5.7 Statutory exemptions/protection

None

5.8 Justification

The ability to manage a network of staff to provide Mental Health First Aid to staff.

6.9 Other risks

Disclosure:

Staff members whilst seeking assistance may submit an email to the mailbox revealing personal information. This email will be deleted once contact is made with the individual and not retained.

Staff members may reveal sensitive information to MHFARs, this information will not be recorded by the MHFAR or the Occupational Health and Safety Branch.

IT Staff access:

IT staff have access to folders but not the files contained, this includes local Information Management Support Officers (IMSO)

6. General Data Protection Regulation (GDPR) Principles

Principle	Compliant – Yes/No	Description of how you have complied
6.1 Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	The Mental Health First Aiders are aware that we will use their workplace information to manage the network and will be used to contact them when directing them to assist someone or to provide communication relating to their voluntary role.
Principle	Compliant – Yes/No	Description of how you have complied
6.2 Principle 2 – purpose limitation	Yes	Staff by way of the procedure and during the conversation will be advised that no personal information will be recorded or held and that it is a confidential service.
Principle	Compliant – Yes/No	Description of how you have complied
6.3 Principle 3 – adequacy, relevance and data minimisation	Yes	Information maintained will be on the Mental Health First Aiders Workplace location details and email address (from Staff directory) and Training information (when course was completed). No personal details will be retained who use the MHFA service.
Principle	Compliant – Yes/No	Description of how you have complied
6.4 Principle 4 – accurate, kept up to date, deletion	Yes	Six monthly checks will be carried out by the branch to ensure MHFARs Database holds the correct workplace information. The MHFARs will be emailed and asked to check that their information is up to date or to advise of changes (i.e where there have

		<p>moved). Staff who no longer wish to be a MHFAr will have their workplace based details moved to a non-active list to allow for reactivation if desired.</p> <p>Reports will be deleted after 3 years</p>
Principle	Compliant – Yes/No	Description of how you have complied
6.5 Principle 5 – kept for no longer than necessary, anonymization	Yes	No personal or sensitive information will be retained on those that use the MHFA service. MHFAs workplace information (as held on the Staff Directory) plus training information will be held to maintain the internal branch network database.
Principle	Compliant – Yes/No	Description of how you have complied
6.6 GDPR Articles 12-22 – data subject rights	Yes	Staff will be able to ask what location and training information is held on them.
Principle	Compliant – Yes/No	Description of how you have complied
6.7 Principle 6 - security	Yes	The Duty holders database is stored on eRDM with only the 4 members of the Occupational Health and Safety Branch having access.
Principle	Compliant – Yes/No	Description of how you have complied
6.8 GDPR Article 44 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	Yes	There will be no data held to be transmitted and no third parties that will have a need for any data transfers.

7. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
No legal basis defined	001	Referred to legal counsel for advice	Eliminated
Personal data and special category for Employees who use the service	002	Delete or anonymize	Reduced
Mental Health First Aiders qualifications auditable	003	System required	Accepted
Sharing health data to protect life	004	Mitigate to public interest in saving a life against disclosing personal details	Reduced

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner

9. Data Protection Officer (DPO)

The DPO may give additional advice, please indicate how this has been actioned.

Advice from DPO	Action

10. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of undertaking the project and formalising the procedure has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	Date each version authorised
Derek Mackintosh Head of Facility Services	02.10.2019



Scottish Government
Riaghaltas na h-Alba
gov.scot

© Crown copyright 2019

OGL

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.scot

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-83960-281-8 (web only)

Published by The Scottish Government, December 2019

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS654082 (12/19)

W W W . g o v . s c o t