



Purpose of this Document

This document has been prepared to inform WMIP members, trustees and agents of the appropriate ways to obtain, hold and process individuals' personal data in compliance with current data protection laws and regulations.

Background

Data protection is a legal requirement for most organisations including WMIP. In May 2018 the General Data Protection Regulation (GDPR) comes into effect.

The Information Commissioner's Office (ICO) web site provides guidance on what must be done to be compliant – see www.ico.org.

Based on the self-assessment questionnaire on the ICO web site WMIP does not have to register with the ICO.

Data Controller

The Chair of the WMIP Board of Trustees will be the "Data Controller".

Data Audit

A data audit should be undertaken to **record and understand**:

- What personal data WMIP holds
- How and when the data was collected
- How the data is moved, processed and accessed within WMIP
- What the data is used for
- If any data is transferred or shared with other organisations
- What security there is for the data
- Any risks there are to the data held

An initial audit was commenced in March 2018. This should be reviewed on an on-going basis – it is NOT a one-off exercise.

Lawful Bases for Holding and Processing Personal Data

Personal data is held for two groups of people:

• WMIP Members and Trustees

• Non-members

Unless otherwise stated, the holding and processing of this data will be done on the following legal basis:

- WMIP Members' and Trustees' data will be used on the basis of "Legitimate Interest" as they have joined WMIP for the purposes of belonging to the organisation.
- Non-Members' data will be held and processed on the basis of "Consent". See the Privacy Notice for Members & Trustees and the Privacy Notice for Non-Members.

Consent

Where consent is required to hold and process personal data it should be collected by clear and informed "opt-in" consent.

The purpose for which the data is required and how it will be used shall be clearly stated on the consent form completed by any individual.

Privacy Notices shall be made easily available whenever consent is obtained either by including a printed statement on the form, or by reference to the WMIP web site or other location to which the individual has easy access to.

Separate consent is required for each purpose for which the data will be used and separate opt-in consent must be obtained for each purpose; for example, by having separate statements with separate tick boxes alongside them.

Consent forms should indicate where and when consent was given.

Consent forms should also indicate that an individual can withdraw their consent at any time.

Reference to the Privacy Notices should be adequate for this purpose for the data which WMIP holds.

Opt-in consent should be time limited and renewed from time-to-time.

WMIP Events Data

Personal data collected in relation to WMIP events will be kept for a period of six years after the date of the event.

The data will be kept for two purposes:

- To record attendance (administration, H&S and CPD records)
- To indicate permission to include a person's contact details in WMIP's mailing list

Booking Forms

Booking forms should refer to WMIP Privacy Notices which can be viewed on the web site. The form should state that contact details are required for administration of the event. A separate box should be included to gain consent to add non-member's contact details to our events mailing list; if left blank then consent is not given.

Attendance Sheets All people attending a WMIP event should have their name and contact details

on a list of attendance. This is for H&S requirements in case of an emergency at the venue. A separate box should be added to the attendance sheet requesting permission to add the contact details of non-WMIP members to the WMIP mailing list for future events. This box must be left blank for the attendee to tick or sign to demonstrate their opt-in to being included on the mailing list. Attendees at events should complete the attendance sheet to record their attendance. They should separately confirm their opt-in to the mailing list by ticking or signing an optional box.

Individuals' Rights

Individuals have specific rights over their personal data:

- To be informed what data is collected and how it will be used
- To have access to the personal data WMIP holds about them
- To have errors in the data corrected within one month
- To object to the processing of their data

WMIP should provide a copy of this data if requested within one calendar month free of charge.

Duplicate copies can be charged at cost.

Reasonable identity checks should be made to ensure that the individual requesting access to the data is who they say they are before the data is supplied. If no longer required the individual can request that their personal data is erased; however, data can be retained if there is a "legitimate interest" or legal/regulatory requirement. There are other rights which generally do not apply to the data held by WMIP; for example, restriction of processing, portability and automated decision-making and profiling.

Accountability and Governance

Any person collecting or processing personal data within or for WMIP shall take all reasonable steps to keep the data secure.

- Paper records should be kept in a locked location.
- Electronic records should only be held in password protected files.
- If personal data is stored on a computer or server to which other people have access, only people with appropriate access rights shall be able to access the files.
- Data should not be shared with third parties or transferred outside WMIP and its contracted administration agency at any time.

The principles set out in this document shall form part of any contract with an outside person or agency which collects, stores and/or processes the data on behalf of WMIP. Any such person or agency shall have in place appropriate data security policies and procedures. WMIP shall maintain a risk register to cover all personal data held. Where a risk is identified a mitigation plan shall be put in

place and implemented.

WMIP holds only limited personal data and nearly all of this is for the legitimate interests of the organisation as set out in the articles of association. By the nature of the data held and processed, it is not considered necessary to appoint a named Data Protection Officer for WMIP.

Reporting Data Breaches

It is not considered necessary to make a formal report in the case of a data breach for nearly all the data which WMIP holds. The only data which potentially, if breached, would need to be reported are the records held by the ethics committee when considering a grievance. If this data is breached it should be reported to the individual and to the ICO.