Data Protection Policy

Introduction

In May 2018, the General Data Protection Regulations were introduced dealing with personal information. Personal information is any such information from which it is possible to identify an individual. The Friends of the Intelligence Corps Museum (hereafter FICM) is required to comply with these regulations. This Policy sets out the information which FICM will process as part of its legitimate interests, specifically the protection of personal information for membership and communication purposes.

Aim

The aim of this Data Protection (DP) policy is to ensure that FICM:

- Protects the rights of members
- Complies with DP law and follows good practice
- Is open about how it stores and processes members' data
- Eradicates, or minimises, the risks of a data breach

It also stipulates how personal information will be acquired, stored, processed, shared and destroyed in line with DP principles and individuals' rights, which are found at Annex A to this Policy.

Information

The following section defines how personal information, including photographs, will be acquired, stored, processed, shared and destroyed.

Where group photographs are being taken members will be asked to step out of shot if they do not wish to be in the photograph that may be publicised. General consent will be obtained verbally from member(s) in the photograph(s) and members will be informed as to where photographs will be displayed. Should a/the subject of the photograph require, this consent will be in writing, which will be retained.

Should a member wish at any time to remove their consent and to have his/her photograph removed then he/she should contact the Membership Secretary, or any Trustee of the Charity, to advise that the photograph is no longer to be displayed. See "Removal of Consent" below.

<u>Acquisition:</u>
Information will be obtained primarily from those wishing to become members of FICM, they will be asked to provide information that is relevant for membership purposes. This will include:

- Name
- Postal address
- Email address
- Telephone number/s
- Gift Aid entitlement
- Bank account details (where using bank facilities for subscription / event payments)

Where additional information may be required, this will be obtained with the consent of the member, who will be informed as to why this information is required and for which purpose it will be used.

Members must inform the FICM Membership Secretary if any of their personal information changes to ensure FICM holds the correct and current contact information.

Storage:
Information will be stored ideally in electronic form, mainly in the Membership Database, held by the FICM Membership Secretary. Any device on which such information is held will be password-protected; such devices include Desktop Computer, Laptop, Tablet/iPad, Smartphone and also includes external storage devices such as DVD, CD, Flash Drives, backups. Hard-copy material will be stored in a secure container.

Processing:
The FICM Board of Trustees will ensure that member information is used appropriately.

Appropriate use of information provided by members will include:

- Communicating with members about FICM events and activities.
- Communicating with members about membership and/or renewal of membership
- Communicating with members about specific issues that may have arisen during their membership

Inappropriate communication would include sending FICM members marketing and/or promotional materials from external service providers and/or revealing individual's personal information to those not authorised to receive it.

Sharing:
Personal information may be shared internally or externally:

Internally:

- to Trustee Board members – as required to facilitate member's participation in FICM activities

Externally:

- for products or services, such as direct mailing of the Sub Rosa newsletter or
- If FICM has a statutory duty to disclose it for other legal or regulatory reasons

Where a member's information has to be shared outside of FICM, other than for the reasons above, the member's consent will be sought (where appropriate). The member will be informed with whom the information will be shared and for what reason.

Destruction:
Membership information has to be retained so that services can be provided to FICM members. In most instances, information about membership will not be stored for longer than 12 months after a member leaves FICM. The exceptions to this are

- When a member withdraws consent for the use of his/her information and
- When there may be legal or insurance circumstances that require information to be held for longer, whilst the issues or investigations are resolved. Where this is the case member/s will be informed how long the information will be held for and when it is deleted – if these details are known and it is appropriate for this information to be revealed.

Removal of Consent:
A member may withdraw his/her consent for FICM to use their personal information at any time. The member should request, ideally in writing or email, either the Membership Secretary, or any Trustee of the Charity who will forward the request to the Membership Secretary immediately. The information will be destroyed and a record made of that destruction. All storage, whether hard-copy or electronic (including backups) will be destroyed.

Members should be aware removing consent for FICM to process their information will, effectively end their membership. Any routine instructions a member may have with their bank, benefitting FICM, should also be cancelled should consent be removed.

Accountability and Governance

The FICM Board of Trustees is responsible for ensuring that FICM remains compliant with data protection requirements and can evidence that it has. Where consent of a member is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely.

The Secretary to the FICM Board of Trustees will ensure that new Trustees joining the Board receive an induction into the requirements of GDPR and the implications for their role. Board Members shall also stay up to date with guidance and practice within.

The Board will review DP and who has access to information on a regular basis as well as reviewing what data is held. When Trustees relinquish their roles, they will be required either to pass on data to those who need it, to the successor in their role, and/or to delete data.

Data Breach Notification

In the event of a data breach, action shall be taken to minimise the harm. This will include:

- assess the severity of the breach,
- reporting a serious breach to the Information Commissioner's Office,
- contacting the relevant FICM members to inform them of the data breach and actions taken to resolve the breach,
- ensuring that all FICM members are made aware that a breach has taken place, how the breach occurred, what actions have been taken to resolve the breach and what has been done to prevent a subsequent breach.

The FICM Board of Trustees shall seek to rectify the cause of the breach as soon as possible to prevent any further breaches.

Where an FICM member feels that there has been a breach by FICM, a Board Trustee will ask the member to provide an outline of the breach. If the initial contact is by telephone, the Board Trustee will ask the FICM member to follow this up with an email or a letter detailing their concern. The alleged breach will then be investigated by members of the Board who are not in any way implicated in the breach. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Member Access Request

Each FICM member is entitled to request access to the personal information that is held on him/her by FICM. The request needs to be received in the form of a written request to the Membership Secretary. The request will be formally acknowledged on receipt and dealt with expediently (*), unless there are exceptional circumstances preventing this action. FICM will provide a written response detailing all information held on the member. A record shall be kept of the date of the request and the date of the response.

(*) legislation requires that information will generally be provided within one month

Review of this Policy

The policy is reviewed on an annual basis by Trustees of FICM at their full Board Meeting held in the Spring to ensure continuing compliance. It will further be reviewed in light of any change to legislation or in the event of a data breach.

This Policy was last reviewed by the FICM Board of Trustees in May 2020. The next review is scheduled to be held in May 2021.

01 May 2020