Imago Mundi CIO

Data Protection Policy and Procedures

(Approved by the Board on xxxx 2026)

The primary purpose of this policy is to protect trustees and other persons against possible misuse of information held about them by Imago Mundi CIO (hereafter the Organisation). It is written to comply with the Data Protection Act 1998 and the General Data Protection Regulation 2018. The policy seeks to apply guidance from the Information Commissioner's Office to the data processing activities of the Organisation.

The policy applies only to personal data relating to a living individual who can be identified from the data, either on its own or in combination with other information. The policy recognises that some data may be particularly sensitive due to its implications in a social context and therefore obtaining, recording or holding it requires extra care. If the Organisation takes possession of personal data, it becomes its controller and therefore legally responsible for it, even if it is processed on the Organisation's behalf by another organisation.

The Organisation is a Charitable Incorporated Organisation engaged in promoting and extending interest in the academic history of cartography, maps and mapping worldwide. It also oversees the production of the journal 'Imago Mundi: The International Journal for the History of Cartography' and co-ordinates the biennial series of International Conferences in the History of Cartography. It obtains, holds and deals with personal data solely for these purposes.

The Organisation's processing of personal data that comes under its control must respect the eight principles defined by the Regulatory framework. Accordingly:

1. First principle: personal data must be processed fairly and lawfully

1.1 Policies

The Organisation should tell people in advance what it intends to do with their data.

The Organisation must use the data in ways that people would reasonably expect.

1.2 Procedures

Where the Organisation gathers data from anyone, including non-Trustees, in pursuit of its objectives it will ensure consent is given to use data and will provide an accurate explanation of how the data has been and is used.

The election of a Trustee should be accompanied with a written notice explaining what the Organisation will do with Trustees' data.

This explanation about the use of data should be summarised and repeated on other relevant documents, to ensure that the way data is processed is regularly drawn to each Trustee's attention.

The notice should make clear that election will be deemed to constitute agreement to the uses thus defined.

2. Second principle: Personal data shall be obtained only for specific purposes and shall not be used for a purpose incompatible with the purposes for which it was collected.

2.1 Policies

Trustees' personal data shall be used solely for managing their trustee status, or, for example, invitations to events mounted or sponsored by the Organisation.

Personal data may be used for statistical or reporting purposes but, if so, must be summarised or rendered anonymous in such a manner that no individual can be personally identified.

Personal data may not be shared with any third party except when necessary in connection with matters such as, for example, processing banking Direct Debits or Gift Aid reporting.

If the Organisation wishes to use personal data in any other way, appropriate consent from the person in question should normally be sought and obtained. If the proposed use involves disclosure to a third party, obtaining consent is mandatory.

2.2 Procedures

Judgments about the uses of personal data for purposes that might be considered marginal to the policies should be recorded on behalf of the Board of Trustees.

Consent notices should be drafted so as to ensure clear communication and with a prominence appropriate to the matters on which consent is sought.

3. Third principle: Personal data obtained should be adequate, relevant and not excessive in relation to the purposes for which it is processed.

3.1 Policies

Personal data of trustees should normally be held solely to facilitate communication within the Organisation.

Personal data should be limited to neutral, factual, non-judgmental information and held within a unique personal profile.

The Organisation should not obtain or hold any 'sensitive' personal data about individuals.

The Organisation should not retain individuals' financial details, except as necessary for such purposes as processing Direct Debits or Gift Aid.

All reasonable precautions should be taken to avoid including personal data in email or other correspondence. Where inclusion is required, for example email or postal addresses, its use should be anticipated in the Organisation 's data processing notices.

3.2 Procedures

The contents of a unique personal profile should normally be limited to the following information:

Login name
Password
Full name and preferred salutation
Email address (and website address, if applicable)
Postal address
Telephone (and fax, if applicable)
Date of becoming a Trustee/joining the Organisation
Direct Debit and Gift Aid status

In the event that any other person wishes for access to any personal profile information, for example to contact an individual, the permission of the individual should be sought.

4. **Fourth principle: Personal data should be accurate and kept up-to-date**.

4.1 Policies

Trustees should be encouraged to keep the Organisation up-to-date with changes or corrections known to them, particularly in respect of their personal profiles.

Changes and corrections should be implemented promptly, whether these are notified by trustees or identified by the Organisation.

Due care to respect the Organisation's policies and ensure accuracy should be applied to entering new data or updating existing records and in creating new files or templates.

4.2 Procedures

Encouragement to trustees to review their personal profiles should be compatible with procedures such as those set out in paragraph 2.1. above.

The administration should employ means for checking, ideally automatically, that notified changes are captured and processed promptly.

The checking should include flagging inappropriate changes, for example in the quality of data to be added, to allow exercise of appropriate policy judgments.

5. Fifth principle: Personal data should not be held for longer than required for the purposes for which it is obtained

5.1 Policies

The retention of a trustee's personal information should be limited to the term of service as a trustee and a reasonable time thereafter, as needed to maintain or renew contact at a later date.

Financial information should not be retained beyond the time needed to process the transaction for which it is provided, in particular, the Organisation should neither collect nor retain credit card data.

5.2 Procedures

The preferred retention period for individual trustee records is currently

Trustees: retained while active. Resigned or died: archived for three years against possible renewal, then deleted.

If reasons of Regulation, business purposes or historic interest arise for longer retention, an opinion from the Board of Trustees should be sought.

Trustee names and dates of membership may be archived to facilitate renewals of contact, should they occur.

6. Sixth principle: Personal data should be processed in accordance with individual rights under the Regulations

6.1 Policies

Individuals are entitled to access all personal data held about them, which will normally be the information in their personal profiles, as identified under the third principle.

Personal data should not be held outside individuals' personal profiles, particularly in emails, unless it is contained in correspondence with the individual to which the individual has received the whole string of messages.

Individuals should be encouraged to access their personal profiles, particularly to verify that it is complete, accurate and up-to-date to their satisfaction and as a means for the administration to be confident that this is so.

The Organisation does not use individuals' personal information for the purposes of direct marketing. Should this policy change in the future, prior consent should be obtained from each individual targeted.

6.2 Procedures

7. Seventh principle: Appropriate technical and organisational procedures should be taken to prevent unauthorised processing and against accidental loss, damage or destruction.

7.1 Policies

The Organisation's data security should provide protection against deliberate, accidental and careless processing, in particular of any personal data that might be used to facilitate identity theft or other misuse.

The Organisation should restrict personal data held by it to avoid retaining data that might cause harm to the people affected if there were to be a security breach.

7.2 Procedures

The Organisation seeks to mitigate the risks to individuals of harmful breaches of data security through its data collection policies described under the previous principle. In particular, the Organisation seeks to minimise any holding of personal financial information or non-public identifiers and to avoid holding any 'sensitive' date that might cause harm if revealed by a data breach.

Access to the Organisation's computer and the online servers that its applications use is restricted to authorised users and is protected by means of multiple passwords. The Organisation installs on a timely basis the routine security updates issued by application providers.

The Organisation's procedures require regular backups of data held separately from the Organisation's computer.

The Organisation does not store personal data on memory sticks. If it were to encounter a need to do so, the data would be encrypted.

8. Eighth principle: Personal data should not be transferred outside the European Economic Area unless the recipient country provides an adequate level of protection for personal data.

8.1 Policy

The Organisation should not transfer personal data outside the EEA, except as this may occur in their independent processing by way of its major service providers such as its bankers and others who have their own responsibilities as data controllers.

8.2 Procedures

Changes in trustees' personal data in the membership database should be initiated by the Organisation's administration or directly to their personal profiles by trustees.

Notice to appear in trustees' election notice

Data Protection

In agreeing to become a trustee of Imago Mundi CIO, you consent to us using the information we may hold about you for the purposes of administration and to correspond with you on matters concerning Imago Mundi CIO. This information will not be used for any other purpose nor communicated to any third party without your consent. The information will be recorded in your trustee profile, to which you have access through the Hon. Secretary. You are invited to use this access to satisfy yourself that it is accurate and up-to-date.

Other notices should be compatible with the one above.