INTERNATIONAL ORTHOPTIC ASSOCIATION

2018

IOA POLICY FOR:

International Orthoptic Association

www.internatiaonalorthoptics.org

1/1/2018

INTRODUCTION

The IOA needs to gather and use certain information to provide our members with the benefits of membership in our association and to, work with our volunteers and with those with whom we collaborate with. This requires data to be collected and processed. As an organization we adhere to this principle: When storing and transmitting data, we must ensure a high level of data protection and data security.

We view it as our duty, as an international charitable organization, to comply with the various legal regulations around the world that govern the collection and processing of personal data. Our top priority is to ensure universally applicable, worldwide standards for handling personal data. For us, protecting the personal rights and privacy of each and every individual is the foundation of trust in our relationships.

Our Data Protection Policy lays out the requirements for processing personal data to ensure, as much as possible, that it is kept safe and secure. It meets the requirements of the European Data Protection Directive and ensures compliance with the principles of national and international data protection laws in force all over the world. The policy sets a globally applicable data protection and security standard for our Association.

CONTENT

KEY DETAILS

Policy Prepared By: IOA President, Karen McMain, and reviewed by IOA President Elect, Jan Roelof Polling & Deborah Brett, Partner, Commercial and Regulatory Law, Blandy & Blandy LLP

Approved By IOA Council of Management: May 18, 2018

Policy Became Operational On: May 18, 2018

Next Review Date: May 18, 2020

Purpose

This data protection policy ensures the IOA:

- complies with data protection law and follows good practice
- protects the rights of our members
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

Scope

1. This policy applies to all individuals who hold IOA voluntary positions, who serve on IOA committees and contractors who are employed by the IOA.
2. This policy describes the organization's requirements regarding maintaining the protection of IOA personal data.
3. It applies to all data that the Association holds relating to identifiable individuals. This can include:
    - Names of individuals
    - Postal addresses
    - Email addresses

- Telephone numbers
- …plus any other information relating to individuals

4. The IOA holds two types of information which are covered by this policy
    - association information – publicly available information about the association, its officers and Council of Management Members, their contact emails for public use and some confidential information regarding officers and Council members personal information – such as telephone numbers, addresses, job titles, our collaborators names, titles and addresses and our members names and emails and volunteers, exchange visitors, host sites and award nominees, names, addresses, and titles.
    - Highly sensitive data is **NOT** processed by the IOA.

Data Protection Principles

The European Union (EU) General Data Protection Regulations (GDPR) set out the eight principles with which the IOA must comply whenever it processes personal data. Whenever processing information about data subjects the IOA will apply the following eight data protection principles:

1. Personal data will be processed fairly and lawfully
2. Personal data will be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required
4. Data should be accurate and kept up-to-date
5. Data should not be kept for longer than is necessary for purpose
6. Data processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organizational measures should be taken unauthorized or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the European Economic Area unless that country or territory ensures an adequate level of data protection.

Definitions

Term: Data Controller

Definition: Data Controller for this policy is the person who jointly determines with the IOA Council of Management the purpose for which and the manner in which personal data are, or are to be, processed.

Term: Data Protection Incidents

Definition: Data protection incidents are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by third parties or IOA volunteers.

Term: Data Subject

Definition: Data subject under this Data Protection Policy is any natural person whose data can be processed. In some countries, legal entities can be data subjects as well.

Term: General Data Protection Regulation (GDPR)

Definition: The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Term: Highly Sensitive Data

Definition: Highly sensitive data is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership, physical and mental health or conditions, ones sexual life, or information that relates to a criminal offence of a data subject.

Term: Personal Data

Definition: Personal data is any information related to a person that can be used to identify the person, including a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Term: Processing

Definition: Processing personal data means any process, with or without the use of automated systems, to collect, store, organize, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media.

Data Protection Risks

This policy helps to protect the IOA and its members from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the Association could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who volunteers for the IOA has some responsibility for ensuring data collected is stored and handled appropriately.

Each committee which handles personal data must make sure it is handled and processed in line with this policy and data protection policy.

However, these people have key areas of responsibility:

The IOA officers and its Council of Management members are ultimately responsible for ensuring the IOA meets its legal obligations.

The IOA President is responsible for:

- Keeping IOA Officers, Council Members, Committee Chairs and the Coordinator of IOA Volunteers updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies in line with an agreed schedule
- Arranging data protection training and advice as needed for IOA Council members
- Providing refresher training at regular intervals for existing IOA personnel
- Handle protection questions from Council members and IOA officers and anyone else covered by this policy
- Dealing with the requests from individuals to see the data the IOA holds on them (subjects access requests)

The Oversight Committee and the Local Organizing Committee is responsible for:

- Checking and approving any contracts with third parties which handle the IOA's sensitive personal data related to Congress registrations, abstract submissions and exhibitor and sponsorship contact information. They will seek legal advice when indicated.

The Data Officer (IOA Secretary) is responsible for:

- Dealing with requests from individuals to see data the IOA holds about them (so called subject access requests)
- Dealing with data protection inquiries from IOA members who hold IOA positions and serve on IOA committees.
- Notifying the Information Commission Office of breaches of IOA data protection

The IOA Web Master and IOA Coordinator of Operations Management are responsible for:

- Ensuring all systems used for IOA web hosting and web programming meet acceptable security standards
- Performing regular checks an scans to ensure security software and hardware is functioning properly

General Procedures

This document sets out guidelines in a number of specific areas where particular attention should be paid in order to help protect the confidentiality of personal data held by the IOA. There are, however, a number of general procedures which for those who volunteer for IOA positions and or committees should follow:

- We will only hold information for specific purposes. We will inform data subjects what those purposes are. We will also inform them if those purposes change.
- The only people able to access data covered by this policy should be those who **need it for their IOA work**.
- Data **should not be shared informally**.
- The IOA **will provide training** to all IOA volunteers to help them understand their responsibilities when handling data.
- Individuals who end their term of office in an IOA position **will be removed** immediately from mailing lists and access control lists

- Contractors, consultants and external service providers employed by the IOA will be subject to strict procedures with regard to accessing personal data by way of **formal contract** in line with the provisions of the Data Protection Acts. The terms of the contract and undertakings given will be subject to review and audit to ensure compliance
- The IOA will carry out an **annual review** of our data protection policy and procedures

IOA volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Association or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- IOA volunteers **should request help** from their IOA President or officers if they are unsure about any aspect of data protection.

Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purpose. It must not be further processed in any manner incompatible with those purposes.

IOA process Personal Data for the following purposes:

1. To provide access to the members only section of the IOA website
2. To confirm IOA membership so reduced IOA Congress rates can be provided
3. To provide members with information on IOA Congress registration deadlines, abstract submission deadlines and Congress meeting news
4. To process applications for IOA awards and education grants
5. To provide IOA members with important news related to the orthoptic profession
6. To provide IOA members with access to newsletters from organizations in which the IOA holds membership in
7. To process applications for IOA volunteer, exchange and host programs
8. To invoice and collect subscriptions from members associations and individual members

9. To contact IOA officers, Council of Management members and IOA volunteers to carry out IOA business
10. To fund raise for IOA charitable pursuits
11. To process donations and bequeaths
12. To comply with our legal obligations as a UK charity to submit a list of our members annually to the Companies House

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

Data Storage

These rules describe how and where data should be safely stored.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- IOA volunteers should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between IOA volunteers. Ideally passwords should contain upper and lower case letters, a number and a symbol.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

- We will make sure all portable devices – such as memory sticks and laptops – used to store personal information **are encrypted**
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **security software and a firewall**

Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

IOA will not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

IOA will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

IOA will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all IOA's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

IOA will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Fair Processing Notice.

Data Use

- Personal data should be handled in such a way as to restrict access only to those persons with an IOA business reasons to access this information.
- When working with personal data, IOA volunteers should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**.
- Personal data should **never be transferred to organizations, states or countries that do not have adequate data protection policies.**
- IOA volunteers **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymized in accordance with IOA's data retention guidelines.

Data Accuracy

The IOA will take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort IOA should put into ensuring its accuracy.

It is the responsibility of all IOA volunteers who work with personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. IOA volunteers should not create any unnecessary additional data sets.
- IOA volunteers should **take every opportunity to ensure data is updated.** For instance, by confirming a members details when they make contact.
- The IOA will make it **easy for data subjects to update the information** the Association holds about them. For instance, via the Association's website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a member can no longer be reached on their stored email address, it should be removed from the database.

Data Subject Rights

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold (discussed below);
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling;
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask or their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above.

You must immediately forward any Data Subject request you receive to the Data Officer (IOA Secretary).

Subjects Access Requests

All individuals who are the subject of personal data held by the IOA are entitled to:

- Ask **what information** the Association holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the IOA requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller (IOA Secretary).

The data controller will aim to provide the relevant data within 40 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data For Other Reasons

In certain circumstances, personal data will be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the IOA will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the IOA President and its board and from the IOA's legal advisers where necessary.

Providing Information

The IOA aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the IOA has a privacy statement, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the IOA's website]

Data Protection Incidents

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

All individual who hold IOA voluntary positions, who serve on IOA committees and contractors employed by the IOA must inform the IOA President and Secretary (Data Controller) immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents).

In cases of
» improper transmission of personal data to third parties,
» improper access by third parties to personal data, or
» loss of personal data
The IOA will immediately report such incidents to the appropriate authority as required under the GDPR.