USA Deaf Sports Federation
www.usdeafsports.org

Policy:	Data Collection Policy
Date Issued:	August 2022
Owner:	Governance
Applies to:	USADSF Board and staff, NSOs, NSCs, volunteers, athletes, and other Persons as specified in this policy

Purpose: This policy describes how this personal data must be collected, handled and stored to meet the USADSF data protection standards as well as legislative requirements.

This data protection policy ensures USADSF:

- Complies with data protection law and follows good practice
- Protects the rights of individuals
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Policy Statement: USADSF gathers and uses certain information about individuals; athletes, coaches, board members, volunteers, customers, suppliers, business contacts, employees, and other people the USADSF has a relationship with or may need to contact.

This data protection policy ensures USADSF:

- Complies with data protection law and follows good practice
- Protects the rights of individuals
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

It applies to all data that the USADSF holds relating to identifiable individuals, even if that information technically falls outside of the state and federal law. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- Birthdates;
- Gender;
- Race/Ethnicity;
- ICSD assigned identifier (ICSD ID);
- Audiogram and relevant information;
- International competition participation; and

- Any other information relating to individuals.

Data collection requirements change from time to time based on new and revised laws. The list provided above is not exhaustive and only includes a basis for the type of information managed through the USADSF.

Privacy and Data Collection Law

The state and federal laws describe how organizations including USADSF must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The state and federal laws are generally underpinned by seven important principles, that data:

- Be processed fairly and lawfully.
- Be obtained only for specific, lawful purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Not be held for any longer than necessary.
- Processed in accordance with the rights of data subjects.
- Be protected in appropriate ways.

Data Protection Risks

This policy helps to protect USADSF from some very real data security risks, including:

- Breaches of confidentiality: information being given out inappropriately.
- Failing to offer choice. All individuals should be free to choose how the USADSF uses data relating to them.
- Reputational damage. The USADSF could suffer if external parties successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with USADSF has some responsibility for ensuring data is collected, stored and handled appropriately. Anyone who handles personal data must ensure that it is handled and processed in line with this data protection policy.

However, the following members have key areas of responsibility:

- The USADSF Governing Board is ultimately responsible for ensuring that the organization meets its legal obligations.
- The Information Technology Overseer is responsible for:
    - Providing data protection training and consultation for the USADSF Governing Board and the people covered by this policy.
    - Responding to requests made by individuals to access their data in the USADSF system (also called ‘subject access requests’).

    - Reviewing and making recommendations to the Governing Board for any contracts or agreements with third parties that may handle and/or store the USADSF's sensitive data (i.e. cloud computing services) ;
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Keeping the USADSF website accessible for any changes to be made by staff.
- The head of Marketing, Development and/or Public Relations is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, staff/employees (staff) should request it from their immediate supervisors.
- USADSF will provide training to all staff to help them understand their responsibilities when handling data.
- Staff should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the USADSF 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 with care.
- Staff should request help from their immediate supervisors or IT Overseer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Overseer. When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see or access 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.

- Staff should make sure paper and printouts are not left where unauthorized people could see or access 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 unauthorized access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared between staff.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated media, drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure and remote location, away from general office space.
- Data should never be saved or downloaded directly to devices, i.e. desktops, laptops, tablets, smartphones, etc. However, the process of transfer to cloud is an exception for downloading to devices. The downloaded data must be removed from devices and/or non-designated locations immediately after the transfer process.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is of no value to USADSF unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, staff should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT Overseer shall consult how to send data to authorized external contacts.
- Staff should not save copies of personal data to their own computers. Always access and update the central copy of any data.

USADSF will not sell and/or share personally identifiable information (PII) with any entities or individuals outside the USADSF. PII defines as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a member, U.S. citizen, lawful permanent resident, or employee or contractor to the USADSF.

Data Accuracy

The law requires USADSF to 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 USADSF should put into ensuring its accuracy.

It is the responsibility of all staff who work with 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. Staff should not create or duplicate any unnecessary data sets.
- Staff should take every opportunity to ensure the data is updated as soon as notification is made to the staff by a member via writing (i.e. e-mail or text).
- Data should be updated as soon as inaccuracies are discovered. For instance, if a member can no longer be reached on their stored telephone number or email address, it should be removed from the database.

Subject Access Requests (SAR)
All individuals who are the subject of personal data held by USADSF are entitled to:

- Ask what information the organization 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 organization is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request, SAR.SAR from individuals should be made through an email.

The USADSF will aim to provide the relevant data within the 30 days of a SAR. The USADSF will always verify thentity of anyone making a subject access request before releasing any information.

Disclosing Data for Other Reasons
In certain circumstances, the state and federal law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, USADSF will disclose requested data. However, the IT Overseer will ensure the request is legitimate by seeking assistance from the Governing Board and the USADSF's legal advisers where necessary.

Disposal of Data
USADSF will only dispose of data and records in accordance with the requirements of the state and federal regulations. However, records will be retained as provided in the Data Retention Schedule.

Data must not be destroyed if it is, or may be, the subject of a subpoena, or other formal request for access or relate to any ongoing action such as an appeal, regardless of whether the minimum statutory retention period has expired.

Data Retention Schedule

All staff members have the responsibility for identifying and retaining records in accordance with established criteria and guidelines as outlined in the Data Retention Schedule below.

Beyond the identified below any record or document that may have historical or enduring value should be reviewed by the Governing Board prior to any destruction.

Type of Record	**Duration**
Disciplinary records - Code of Conduct	Permanent
Passport - Text	Immediate after arrival from international competition
Passport - Photo	Immediate after approval
Code of Conduct	18 months after international competition
Audiogram	Permanent
Health Record	3 months after international competition
Conflict of Interest	1 year from date of signature
Meeting Minutes	Permanent
Audit Reports	Permanent
Bank Statement	10 years
Athlete Participation	Permanent
News Releases	Permanent
Team Rosters	Permanent
Awards	Permanent