# UK Deaf Sport

# Data Protection Policy

| Policy Governance | |
|---|---|
| Last edit date: | July 2020 |
| Review date: | July 2023 |
| Version: | 1 |
| Approved | July 2020 |

**Contents**

## 1. General Principles

This policy defines UK Deaf Sport's (hereafter referred to as UKDS throughout this document) policy in respect of obtaining, storing and using personal information relating to its employees and other stakeholders. It is not contractual but indicates how UKDS intends to meet its legal responsibilities for data protection.

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We regard the lawful and correct treatment of personal information as important to the success of the organisation and to maintaining confidence between those with whom we deal and ourselves. To this end we fully endorse and adhere to the principles of data protection as set out in the Data Protection Act 1998.

The types of personal data that we may process include information about current, past and prospective employees, workers, volunteers including trustees and contractors; participants and members; suppliers and other organisations with whom we have dealings.

This policy applies to all employees, workers, volunteers including trustees and contractors who handle personal data, whether this relates to their colleagues, participants, members or anyone else. A copy will also be given to any third parties to whom we outsource any data processing or storage.

## 2. Data Protection Act

The Data Protection Act (DPA) lays down conditions for the processing of any personal data and makes a distinction between "personal data" and "sensitive personal data" (see Definitions, below).

We endorse and adhere to the eight Principles which are summarised as follows.

Data must:

- be processed fairly and lawfully and shall not be processed unless specific conditions are met
- be obtained only for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- be adequate, relevant, and not excessive for those purposes
- be accurate and, where necessary, kept up to date

- only be kept for as long as is necessary for the purpose(s) for which it was obtained
- be processed in accordance with the rights of data subjects under the Act
- be kept secure from unauthorised or unlawful processing of personal data and protected against accidental loss, destruction or damage to personal data by using the appropriate technical and organisational measure
- not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles apply to obtaining, handling, processing, transportation, and storage of personal data. Employees and agents of UKDS who obtain, handle, process, transport, and store personal data for us must always adhere to these principles.

UKDS will, through appropriate management and strict application of criteria and controls:

- Observe fully the conditions regarding the fair collection and use of personal information
- Specify the purposes for which information is used
- Collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- Endeavour to ensure the quality of the information used
- Ensure that information is held for no longer than necessary
- Ensure that the rights of people about whom information is held can be fully exercised under the Act i.e. the right to be informed that processing is being undertaken, to access one's personal information, to prevent processing in certain circumstances and to correct, rectify, block or erase information that is regarded as wrong information
- Always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or

documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and systems by using secure passwords etc)

- Ensure that personal information is not transferred without suitable safeguards.

The Executive Director has overall responsibility for the management of Data Protection. However, all employees and stakeholders of UK Deaf Sport and agencies and consultancies contracted to carry out work for it are required to abide by the requirements set out in this Policy. All those who manage and handle personal information are to understand that they are contractually responsible for following good data protection practice.

## 3. Definitions

3.1 Personal Data

This is data which relates to a living individual who can be identified from that data, or that data and other information which is in the possession of or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.2 Sensitive Personal Data

Categories of personal data consist of details regarding an individual's racial or ethnic origin; political opinions; religious or other beliefs; membership of a trade union; physical or mental health or condition; sexual life; or criminal proceedings or convictions. This will also include register of ICSD numbers and UKDS membership data.

## 4. Requirements and responsibilities

All personal data will be processed in accordance with the principles of the DPA. Only data to which UKDS is legally entitled to will be obtained and, unless self-evident, the data subject will be advised of the purpose for which it is required.

Sensitive personal data will only be obtained if it is necessary for UKDS to comply with any legal requirements and / or to fulfil any legal obligations it has in connection with the employment of individuals.

Personal data will be obtained and processed only for limited purposes and not in any manner incompatible with those purposes. The extent of personal data obtained and processed will be adequate, relevant and not excessive for the required purposes.

Personal data will be kept up to date, where necessary, and kept for no longer than is necessary for the purpose for which it was obtained. Personal data will be processed in line with data subjects' rights under current legislation. This includes the entitlement, on written request, to see their personal or sensitive personal data held by UKDS on computer or other electronic systems. UKDS may charge a sum, no greater than the statutory maximum, for supplying information under a subject access request. Any person who wishes to exercise this right should make their written request to the Executive Director. We aim to comply with requests for access to personal information as quickly as possible but will ensure that this is provided within 40 days of a receipt of a request, unless there is good reason for delay.

If personal details are inaccurate, they will be amended upon request.

If, by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Unless we are under a legal obligation to release data, or the individual has given us permission, personal information will only be released to whom it relates. Information must under no circumstances be sent outside of the UK without the prior permission of the Executive Director.

Measures will be taken to ensure, as far as is reasonably practicable, security and confidentiality in obtaining, handling, storing and disposal of personal data.

All employees are responsible for ensuring that, if as part of their responsibilities, they collect information about other people, they comply with this policy. Employees are reminded that the DPA does not just apply to records relating to our employees but also to any participant or member file/records. Information stored should therefore be reviewed regularly to ensure it is accurate and up to date. All documents, whether handwritten or stored in emails (current or deleted) are potentially disclosable in the event of a request from an employee or participant/member.

## 5. Employee records

We hold personal information about all employees as part of our general employee records. This includes address and contact details, age, date of birth, employment application details, employment history with UKDS, marital status/civil partnership, details of salary and benefits, bank details, performance appraisals, records relating to holiday, sickness and other leave, working hours and other management records. We may receive and/or retain this information in various forms.

This information is used for a variety of administration and management purposes, including payroll administration, complying with record keeping, facilitating the management of work and employees and other legal obligations.

We also process information relating to employees' health, some of which may fall under the definition of "sensitive personal data". This includes records of sickness absence and medical certificates, DSE assessment and any other medical reports. This information is used to administer company and Statutory sick pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and Working Time Regulations, as appropriate.

Our contracts of employment require the consent of employees to the processing of personal data for the purposes of administration, management and employment.

All employees are responsible for checking that any personal data they provide to us is accurate and up to date, and to inform us of any changes to information previously provided e.g., change of address.

## 6. Data Security

No hard copy personnel files are kept. All records are stored electronically has appropriate levels of authorisation which prevent unauthorised access.

UKDS Managers have access to the personnel records of the employees that directly report to them, but not to files of other employees. Managers may retain their own copies of 1:1 notes or informal discussions with their employees but must not retain their own copies of personal data.

All employees and workers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Information that discloses personal information, including references, will not be provided to any third party without the data subject's prior authority unless it is required or permitted by law, such as the Police, HMRC, Contributions Agency or similar.

Third party processors, such as our outsourced payroll, will be required to provide sufficient guarantees for their data security measures and compliance with them.

We will not collect data that is simply "nice to have" nor use data for any purpose other than what it was provided for originally.

Information that is already in the public domain is exempt from the Act. This includes, e.g., brochures and other sales and marketing aids. Any individual who

has good reason for wishing their details not to be included in such publications should contact the Executive Director in writing.

All employees are responsible for ensuring that information is not kept for longer than necessary. Documents containing any personal information will be disposed of securely and paper copies will be shredded. Information stored on electronic equipment will be erased prior to equipment being sold, disposed of or reallocated.

## 7. Monitoring and review

This policy will be regularly monitored to ensure that it can be applied equally to all employees and stakeholders and updated where appropriate to meet changing legislation and organisational requirements.

This policy is subject to regular review to reflect, for example, changes to legislation or to the structure or policies of UKDS.

Any breach of this policy will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with their manager or the Executive Director.

### Review of this Policy

We keep this Policy under regular review. This Policy was last updated in July 2020.

### Related Documents:

- UKDS Privacy Policy
- Safeguarding Children and Young People Policy
- Safeguarding Adults policy