UK Deaf Sport

Data Protection Policy

The Issue Status

The Issue Status is indicated by the version number in the footer of this document. It identifies the Issue Status of the 'UK Deaf Sport Data Protection Policy'.

When any part of this document is amended, a record is made in the Amendment Log shown below.

The 'UK Deaf Sport Data Protection Policy' can be fully revised and re-issued at the discretion of the UK Deaf Sport Board.

Issue	Amendment	Date	Initials	Policy Owner	Approving Body	Date Approved by Approving Body	Review Date
1.0	First version	July 2020					July 2023
2.0	Revised and updated following BDO Audit. Agreed version	March 2023	DB	JC	UKDS Board	22 March 2023	March 2025
2.1	Addition of section for Board, Committee and Advisory Group Members	August 2024	DB	JC	UKDS Board		
2.2	Section 10 further updated following FARG	September 2024	DB	CR	UKDS Board	September 2024	September 2027

Contents

1. General Principles

1.1 UK Deaf Sport (hereafter referred to as UKDS throughout this document) needs to collect and use certain types of information about employees and/or other stakeholders who come into contact with UKDS, in order to carry out our work. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material.

1.2 The approach taken by UKDS has been put in place to ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019[1].

1.3 This document defines UKDS's 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.

1.4 UK Deaf Sport 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.

1.5 To this end we fully endorse and adhere to the principles of data protection as set out in the Data Protection Act 2018. 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.

1.6 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. The Data Protection Act

2.1 The Data Protection Act (DPA) 2018 and UK GDPR lay down conditions for the processing of any personal data and makes a distinction between "personal data" and "sensitive personal data" (see Definitions, below).

2.2 UKDS intends to ensure that personal information is treated lawfully and correctly. To this end, UKDS will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 2018 (which supersedes the Data Protection Act 1998). The seven principles that form the basis of our data protection framework as set out in the Act are:

[1] As the result of Brexit and with effect from 01 Jan 2021, the UK stopped being part of the EU and hence the "EU-GDPR" ceased to protect the rights and freedoms of UK Citizens regarding their Personal Information. To prevent this becoming the case, the UK Government published an update to the DPA 2018 called the 'Data Protection, Privacy and Electronic Communication (Amendments etc) (EU Exit) Regulations 2019'.

a. **Lawful, fair and transparent processing:** this principle emphasises transparency on how and why data is collected. We will only use personal data in a way that is fair to the individuals and will be honest and open with individuals as to the use of their data.

b. **Purpose limitation:** this principle emphasises the need for all data to be processed for a purpose. We will be clear about our purpose for processing from the start and this will be recorded as part of documentation obligations.

c. **Data minimisation:** this principle emphasises the need for organisations to minimise the data they collect. All data we collect will serve a purpose and we will only store the minimum data required. We will ensure the personal data we process is:
   - *Adequate:* sufficient to properly fulfil our stated purpose
   - *Relevant:* has a link/is relevant to that purpose
   - *Limited to what is necessary:* we will not hold more than we need to for that purpose.

d. **Accurate and up-to-date processing:** this principle requires controllers to ensure the information they hold is accurate and up-to-date and remains so. We will only use data if it remains accurate and relevant. We will take all reasonable steps to ensure the personal data we hold is not incorrect or misleading in any way. If we discover that the personal data is incorrect or misleading, we will take all reasonable steps to correct or erase it as soon as possible.

e. **Storage limitation:** this principle emphasises the need for organisations not to keep data longer than there is a need. We will keep data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Please refer to the data retention and archiving policy for how long personal data and documents need to be retained**.**

f. **Integrity and confidentiality (security):** this principle protects the integrity, privacy and confidentiality of data by placing specific obligations on organisations to secure it. We recognise that we are solely responsible for the security of that data we collect and process and have security measures in place proportionate to the data type.

g. **Accountability principle:** this principle makes the organisation responsible for complying with the UK GDPR and demonstrates compliance. We take responsibility for the processing activities we carry out. To ensure on-going compliance, every step of our GDPR strategy is auditable through the use of policies and procedures.

2.3 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.

2.4 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.

2.5 The Chief Executive Officer (CEO) has overall responsibility for the management of Data Protection. However, all Trustees, employees and stakeholders of UKDS 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. UK GDPR

3.1 UKDS recognises its duties to comply with UK General Data Protection Regulation (UK GDPR). Specifically, UKDS will:

- Secure and document the consent of Individuals prior to collecting any personal data.
- Ensure that individuals understand their rights with regard to the consent that they have given for us to hold and process their data.
- Make it clear that individuals can withdraw their consent for UKDS to hold and process data at any time.
- Not use the data for any purpose other than that for which informed consent is held, except in one of the circumstances outlined in the UK GDPR.
- Ensure that contracts with commissioners and/or funders are clear about information flows and the circumstances in which we will delete data when consent for us to hold and process data is withdrawn by an individual.
- Make the information we hold on an individual available to them upon request and correct inaccuracies in a timely manner.

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

- Observe fully the conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.

- Ensure the quality of information used.
- Ensure that the rights of people about whom information is held, can be fully exercised. These include:

    - The right to be informed that processing is being undertaken.
    - The right of access to one's personal information.
    - The right to prevent processing in certain circumstances.
    - The right to correct, rectify, block or erase information which is regarded as wrong information.
    - The right to erasure.

- Take appropriate technical and organisational security measures to safeguard personal Information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding to requests for information.

4. Definitions

4.1 *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.

4.2 *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.

4.3 *Data Controller*

UKDS is a Data Controller under the Act, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

5. Requirements and Responsibilities

5.1 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.

5.2 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.

5.3 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.

5.4 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 retained in line with the schedule in the Data Retention and Archiving Policy that sets out how long personal data need to be retained.

5.5 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.

5.6 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 CEO.

5.7 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.

5.8 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.

5.9 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.

5.10 Information must under no circumstances be sent outside of the UK without the prior permission of the CEO.

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

5.12 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.

6. Employee Records

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 UKDS 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.

7. Board, Committee and Advisory Group Members

7.1 We hold personal information about all Board, Committee and Advisory Group Members as part of our governance requirements. This includes address and contact details, age, date of birth, Director and/or Advisory Group Member application details, bank details, Board Director appraisals, records relating to meeting attendance and other records UKDS requires to ensure efficient and effective governance arrangements. We may receive and/or retain this information in various forms.

7.2 This information is used for a variety of administration purposes, including administration and payment of expense claims, complying with record keeping requirements, and other legal obligations.

7.3 We may also process information relating to levels of deafness, which falls under the definition of "sensitive personal data". This ensures we can show we are meeting ICSD requirements regarding the percentage of deaf Directors with 55+ decibels hearing loss in their better ear.

7.4 All Directors, Committee and Advisory Group Members are responsible for checking that any personal data they provide to UKDS is accurate and up to date, and to inform us of any changes to information previously provided e.g., change of address.

8. Data Security

8.1 All UKDS information technology devices are fitted with anti-virus software to protect its data from malicious software - known as malware. By installing anti-virus software UKDS will prevent malware attacks that can harm its computers and laptops, steal its data, encrypt it so UKDS cannot access it, or even erase it completely.

8.2 UKDS is aware that data is often at its most vulnerable when on the move. To ensure UKDS data is kept secure, UKDS devices are encrypted to protect confidential information at every stage of its journey, and ensure any files or documents uploaded to the cloud or internal storage hub always remain safe from data loss or theft.

8.3 No hard copy personnel files are kept. All records are stored electronically and have 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.

8.4 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.

8.5 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.

8.6 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.

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

8.8 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 CEO in writing.

8.9 All employees are responsible for ensuring that information is not kept for longer than necessary.

8.10 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.

9. Disclosure

9.1 UKDS may share data with other agencies such as Government Departments, funding bodies and other sporting agencies. Individuals will be made aware of how and with whom their information will be shared.

9.2 There are circumstances where the law allows UKDS to disclose data (including sensitive data) without the data subject's consent. These are:

a. Carrying out a legal duty or as authorised by the Secretary of State.
b. Protecting vital interests of an Individual or other person.
c. The Individual has already made the information public.
d. Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
e. Monitoring for equal opportunities purposes – i.e. race, disability or religion.

9.3 UKDS regards the lawful and correct treatment of personal information as very important to successful working and to maintaining the confidence of those with whom we deal.

10. Monitoring and Reporting

10.1 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.

10.2 Any breach of this policy will be taken seriously and may result in formal disciplinary action.

10.3 The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the ICO. This must be done within 72 hours of becoming aware of the breach, where feasible.

10.4 Any employee who considers that the policy has been breached in any way should raise the matter with their manager or the CEO. If there is a possibility the CEO has breached the policy it should be raised with the Chair.

10.5 Any possible breaches of the policy should be reported as soon as possible to ensure any impact on those whose information is breached is minimised or limited. This will also facilitate decision-making about whether or not UKDS need to notify the Information Commissioner's Office (ICO) or the affected individuals, or both.

10.6 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must also be informed without undue delay.

10.7 Any personal data breaches must be recorded on the UKDS Incident Log regardless of whether the ICO has to be informed of the breach.

11. Review of this Policy

This policy is subject to regular review to reflect, for example, changes to legislation or to the structure or policies of UKDS. The Issue Status table on page 1 of this policy shows the date of the last review, Board approval date and when the next review is due.

12. Related UKDS Documents:

- Privacy Policy

- Cyber Security Policy
- Data Retention and Archiving Policy
- Whistleblowing Policy
- Safeguarding Children in Sport Policy
- Safeguarding Adults in Sport Policy