Dales Pony Society - Data Protection Policy

1 Policy Statement

The Dales Pony Society (DPS or Society) needs to collect personal information to effectively carry out its everyday business functions and activities and to provide its services. Such data is collected from officers, customers, suppliers and members and includes name, address, title, telephone numbers, email address, data of birth, and identification numbers.

It is required to collect and use certain types of personal identifiable information to comply with the requirements of the law, for example EC504/2008 and the 2009 Horse Passports (England) Regulations, however we are committed to processing all personal information in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (GDPR).

The Society's policy is to: collect data for specified, explicit and legitimate purposes only; ensure it is accurate and, where necessary, kept up to date; processed lawfully, fairly, in a transparent manner and in a manner that ensures appropriate security of the personal data; and kept in a form which permits identification of data subjects for no longer than is necessary.

The Society is not registered with Information Commissioners Office (ICO) as it exempt by nature of its activities as a non-profit making charity. The Society recognises the ICO as its Supervisory Authority.

2 Purpose

The purpose is to ensure that the Society meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal information is processed compliantly and in the individual's best interest.

This policy serves as a reference document for officers, volunteers, directors, trustees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

3 Scope

This policy applies to all officers and volunteers with defined roles within the Society, and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 Governance Procedures

4.1 Establishing Compliance

In support of the Policy Statement, the Society has taken action to meet its data protection obligations and to ensure continued compliance with the regulatory requirements. The Society carried out an information audit to enable it to record, categorise and protect the personal data that it holds and processes. It checked for compliance with the data protection laws and its principles and established that data is only processed where the lawfulness of processing has been established and it is kept for as long as is necessary. The Society stores and destroys all personal information, in accordance with the data protection laws, timeframes and requirements.

The Society established that it held no personal data falling within the GDPR's 'special categories'.

The Society has designated an Assigned Person in accordance with the GDPR requirement. The assigned person has an adequate and expert knowledge of data protection law and practices and is fully able to, and capable of, assisting the Society in monitoring internal compliance with the Regulation and to support and advise employees and associated third parties with regards to data protection laws and requirements.

All officers and volunteers know their GDPR obligations and are provided with suitable training in the data protection laws, principles, regulations and how they apply to their role and Society business.

4.2 Principles for Procedures

To to achieve data minimisation, the Society only ever obtains, retains, processes and shares the data that is essential to carry out its services and legal obligations and only keeps data for as long as is necessary. To ensure that only the necessary data is collected, forms have pre-defined fields and only include optional fields for parents or guardians are required to sign on behalf of juniors.

The Society utilises encryption via secret key for transferring personal data to external parties that are within the scope of legal requirement and provide the secret key in a separate format. The legal requirement covers the processing of equine passports. Some personal data is included in the publication of the stud book and show catalogues which are produced for general public information, therefore the data is not encrypted on transmission to the printers.

Restriction access is built into the Society's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose have access to personal information.

Due to the nature of the Society's business, it is sometimes essential for it to obtain, process and share personal information which is only available in a paper format without pseudonymisation options in processing equine passports. It is recognised by DEFRA, the partner Data Processor, that these documents can be transferred using standard postal systems. If for any reason a copy of the paper data must be retained by the Society, we use a physical safe to store such documents as opposed to our standard archiving system.

The Society has established retention periods as set out by the relevant laws, contracts and business requirements. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data at all times. Each procedure defines the retention periods and disposal criteria where relevant. Data is stored for up to 6 years from the date of submission, unless there is a legal requirement to keep the information longer.

4.2 Codes of Conduct and Certification Mechanisms

The Society, is a recognised Passport Issuing Organisation (PIO) number 826020, is not subject to any Codes of Conduct as there are none specified by DEFRA, the Data Controller.

4.3 Third-Party Processors

The Society utilises external processors for certain processing activities. It uses information audits to identify, categorise and record all personal data that is processed outside of the Society, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. External processing is limited to Printing and IT Systems and Services.

The Society obtains company documents, certifications, references and ensures that the processor is adequate, appropriate and effective for the task we are employing them for.

The Society assesses their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance. The continued protection of the rights of the data subjects is the Society's priority when choosing a processor and it understands the importance of outsourcing processing activities as well as its continued obligations under the data protection laws even when a process is handled by a third-party.

Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

5 Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Society. The Society maintains that it does not have any high risk processes or processes that could cause impact to a data subject. The Society would produce DPIA Procedures at the time should the need arise.

6 Data Subject Rights Procedures

6.1 Consent and the Right to be Informed

The collection of personal data is a fundamental part of the services offered by the Society and only processes personal data where there is a legitimate interest.

Where a person wishes to become a member of the Society but does not wish to use services connected with the processing of equine passports, it can only be for the reason to be included on the mailing list for the Society's publications, therefore the personal data is essential for providing this service as a contractual obligation. The personal data required is a precondition of a service we are offering, it is not given as an option and consent is not appropriate.

The Society uses a database for managing membership and equine passports. The personal data held is not available to the general public or other members unless specifically requested by the member. There is a mechanism for managing these member preferences.

The Society recognises that there are six lawful bases for processing and that consent is not always the most appropriate option. The Society has reviewed all processing activities and would only use consent as an option where the individual would have a choice. The Society is therefore not required to have any general procedures for acquiring or managing consent.

6.2 Information Provisions

Where personal data is obtained directly from the individual, the Society provides a Privacy Statement which states what it collects, how, why and when their data is processed, the individual's rights, how to complain and how to get further information.

The Society uses the term Privacy Statement, which is a separate document from its Data Protection Policy and is provided to individuals at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly).

6.3 Personal Data Not Obtained from the Data Subject

The Society has no processes that require personal data from other sources.

6.4 Subject Access Request

Subject Access Requests (SAR) are passed to the Secretary as soon as received and a record of the request is noted. The type of personal data held about the individual is checked to see who else has it has been shared with and any specific timeframes for access.

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

6.4 Officer and Volunteer Personal Data

The Society's policy is that all Officers and Volunteers have to be members of the Society and thus the personal data is restricted to that of members. The Privacy Notice for members informs them of their rights under the data protection laws and how to exercise these rights. .

6.5 Rectification and Erasure

6.5.1 Correcting Inaccurate or Incomplete Data

All data held and processed by the Society is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject informs the Society that the data held is inaccurate, it takes every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The Secretary is notified of the data subject's request to update personal data and is responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject.

Where notified of inaccurate data by the data subject, the Society will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, the Society is unable to act in response to a request for rectification and/or completion, it will provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

6.5.2 The Right to Erasure

Also, known as 'The Right to be Forgotten', the Society ensures that personal data which identifies a data subject is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Society is identified in procedures is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

The Society recognizes that not all personal data can be erased where it is required to be retained by law, in particular, laws and regulations applying to equine Identification Documents.

6.6 The Right to Restrict Processing

The Society has not identified any personal data that would require a data subject request the right to restrict processing. See Section 6.1.

6.7 Objections and Automated Decision Making

The Society does not participate in direct marketing or use personal data in processing for purposes of scientific or historical research and statistics.

The Society does not use automated decision-making processes.

7 Oversight Procedures

7.1 Security and Breach Management

Process procedures are designed to ensure that all personal data held and processed by the Society is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). The procedures have been implemented with adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

7.2 Passwords

Passwords are a key part of the Society protection strategy and are used throughout the Society to secure information and restrict access to systems. It uses a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach.

8 Transfers and Data Sharing

The Society takes proportionate and effective measures to protect personal data held and processed by it at all times, however it recognises the higher risk when data is transferred. Normal postal services are endorsed by DEFRA for situations where data is transferred for legal and necessary purposes for processing equine Identification Documents.

9 Audits and Monitoring

This policy and process procedures document the controls, measures and methods used by the Society to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to this, it carry outs regular audits and compliance monitoring processes that are detailed in the Compliance Monitoring and Audit Policy and Procedure, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Assigned Person has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Council where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Assigned Person and copies provided to the Council and are made readily available to the Supervisory Authority where requested.

10 Training

The Society ensures that all officers and volunteers understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have training and support to ensure and demonstrate their knowledge, competence and adequacy for the role. New and existing Council members, officers and volunteers are trained and supported by: GDPR Training Sessions; coaching; and access to GDPR policies, procedures, and supporting documents. Officers and volunteers are supported and trained in the data protection laws requirements and the Society's own objectives and obligations around data protection.

11 Penalties

The Society understands its obligations and responsibilities under the data protection laws and Supervisory Authority and comprehends the severity of any breaches under the Regulation. Council members, Officers and volunteers have been and will be made aware of the severity of such penalties and their proportionate nature in accordance with the breach.

The Society recognises that: breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher; breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

12 Responsibilities

The Assigned Person, whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its officers, volunteers and Council members and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The Secretary has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Officers and volunteers who manage and process personal information will be provided with data protection training and will be supported to ensure that they are competent and knowledge for the role they undertake.

Appendix A - Definitions

“Consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

“Data controller” means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

“Data processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

“Data protection laws” means for the purposes of this document, the collective description of the GDPR, Data Protection Bill and any other relevant data protection laws that the Society complies with.

“Data subject” means an individual who is the subject of personal data

“GDPR” means the General Data Protection Regulation (EU) 2016/679

“Personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier

“Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

“Recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

“Supervisory Authority” means an independent public authority which is established by a Member State. In the UK this is the Information Commissioner’s Office (ICO).

“Third Party” means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

“Council” means the governing body of the Dales Pony Society consisting of elected Members with the responsibilities of both Directors and Trustees.