



Irish Draught Horse Society (GB)

Registered Charity No. 1080522

Data Protection Policy

No.	Content	Page	No.	Content	Page
1	Introduction	1	8	Document classification and retention	5
2	Legislation	1	9	Third party processors	7
3	How we process personal data	2	10	Data Impact assessments	8
4	Existing safeguards	3	11	Data Subject Rights	8
5	Data breaches	3	12	Governance and oversight	9
6	Council confidentiality	4	13	Appendix A - Definitions	11
7	Training	5	14	Appendix B – Non requirement for Analysis	12

1. Introduction

The Irish Draught Horse Society of Great Britain (IDHS (GB)) needs to collect and store personal information to carry out its everyday business functions and to provide services to the public, in furtherance of the Society's Objects (*Memorandum of Association, paragraph 3*).

Equine data is not covered within this policy because it is not personal data. The confidentiality of veterinary and inspection information is covered by a separate policy document.

Personal data is collected for the following reasons:

- Society membership requires us to collect personal data.
- Personal data is also collected for non-members when they purchase an animal registered with the Society and submit the passport for change of ownership, or when they enter a show where there is no requirement for membership.
- Members of the public often make enquiries which require us to collect basic personal data (name, contact number, email address) in order to respond to their query.
- The Privacy Statement, published on our website, informs the public of their rights under the data protection laws and how to exercise these rights. The Privacy Statement states what it collects, how, why and when their data is processed, the individual's rights, how to complain and how to obtain further information.

2. Legislation

The Society is required to collect and use certain types of personal identifiable information to comply with the requirements of the law, for example the Equine Identification (England) Regulations 2018.

We process all personal information in accordance with the Data Protection Act 2018 (DPA 2018), as amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

The DPA 2018 sits alongside the UK General Data Protection Regulation (UK GDPR), which also came into effect on 01 January 2021.

3. How we process personal data

The IDHS (GB) collects and processes personal data, including titles, names, addresses, telephone numbers, email addresses, dates of birth and membership numbers, from trustees, volunteers, customers, suppliers and members to carry out its functions as defined within the Society's governing documents.

The IDHS (GB) exchanges personal data, limited to names, addresses and when necessary, other contact information such as phone numbers and email addresses with Weatherby's Scientific for the purposes of DNA parentage-testing. Weatherby's Scientific is in the Republic of Ireland.

The IDHS (GB) exchanges personal data with its parent organisation, currently Horse Sport Ireland, also located in the Republic of Ireland. This is required to enable equine passports to be issued and processed and to assist in reducing the risk of passport fraud.

Because we work in partnership with organisations in the Republic of Ireland, we are obliged to adhere to Regulation (EU) 2016/679 of the European Parliament and the Minimum Operating Standards (June 2021) set by Defra.

To remain within the law, personal information that we collect must be:

- Fairly and lawfully processed;
- Processed for limited specific purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with people's rights;
- Kept securely;
- Not transferred to other countries (including into the EU) without adequate protection.

The Society exercises great care in what records we hold about individuals, and how we handle them. Individuals have the right to find out what personal information is held on computer and paper records. This means that any individual with whom the Society has been in contact can request access to personal data held about them.

Should an individual or organisation consider that they are being denied access to personal information to which they are entitled, or that their information has not been handled according to the data protection principles, they can contact the Information Commissioner's Office (ICO) for advice.

Useful information about the Information Commissioner's Office can be found on their website:

<https://ico.org.uk/>

4. Existing safeguards

The Society has been registered with the ICO since 30 October 2001. The registration number is Z5960309. The annual fee is payable in advance on 29 October.

The Society has a Privacy Policy which lists the types of data that we process. This is published on our web site at www.idhsgb.org.uk.

In January 2022, an audit was initiated to record, categorise and protect the personal data that the Society holds and processes, and to verify the rigour of its checking procedures for third-party data processors. As part of this audit, we checked compliance with data protection legislation and principles.

Data is processed only where the lawfulness of processing has been established.

Data is kept only for as long as is necessary. We are committed to storing and destroying all personal information in accordance with the data protection laws, including improved time limits for destruction.

The Society is not a public body and does not hold or process personal data falling within the UK GDPR's 'special categories'.

The guidelines on the ICO website (13/02/2022) confirm that we are exempt from the requirement to have a named Data Protection Officer.

The current trustee members of the Finance and Governance Group of the Council are the Society's data protection team:

Heather Chaplin (Company Secretary)

Jane Imbush (Honorary Treasurer)

James Noble (Society Chair)

Ann Western (Vice Chair)

Group email address: governance@idhsgb.org.uk

The Finance and Governance Group is fully accountable to the Council and the membership and acts in an advisory capacity to support and advise staff, volunteers and associated third parties with regards to data protection laws and requirements;

The Finance and Governance Group will:

- keep data minimisation strategies under review
- explore existing and new technologies to ensure that we are protecting data and individuals to the best of our ability;

The Finance and Governance Group will ensure that adequate and effective records and management reports are maintained in accordance with data protection legislation and internal policies;

The Finance and Governance Group has an action plan to deal with document retention and secure destruction.

5. Data breaches

The Society has a duty to protect all its members from breaches of privacy and confidentiality. The consequences of personal data loss to individuals can be massive. It can lead to fraud, identity theft, litigation and considerable personal distress. The consequences to the Society are also potentially very damaging, as heavy fines can be imposed for any breach of data protection regulations as well as an adverse impact on its reputation.

It is therefore extremely important that all our trustees, staff and others who carry out tasks on behalf of the Society understand their responsibilities under the data protection legislation. All trustees, staff, volunteers, judges, inspectors, third-party contractors and other officials must agree in writing to adhere to the Data Protection Policy before they can begin to work with the Society.

Action to be taken in the event of a data security breach:

The Council	The Council must have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether there is a need to notify the relevant supervisory authority or the affected individuals, or both.
Trustees, staff and volunteers	Anyone who detects a breach or possible breach of personal data relating to the Society's members and customers must inform the Finance and Governance Group immediately.
Finance and Governance Group	The Finance and Governance Group will: <ul style="list-style-type: none"> • meet to carry out a risk assessment and implement the action plan; • Within 24 hours of the data breach, a member of the Finance & Governance Group will ascertain from the Information Commissioner's Office website whether the matter needs to be reported and if necessary, report it; • Where there is a risk that the breach may adversely affect individuals' rights and freedoms, the Finance and Governance Group must ensure that those individuals are informed without undue delay. • Report the matter to the Council.
Record keeping	The Finance and Governance Group must keep a record of any personal data breaches, regardless of whether there was a requirement to notify the ICO.

6. Council confidentiality

Trustees must sign a confidentiality agreement before they take up their posts on the Council. The requirement for confidentiality extends beyond the trustee's term of office.

Breaches of Council confidentiality are a disciplinary matter.

Any persons who volunteer to help at inspections, the National Championship Show and other events where they have to handle personal data must receive training in how to safeguard such data.

They must also sign a confidentiality agreement to show that they understand the responsibilities of their role and the importance of confidentiality.

All trustees (and volunteers) who encounter personal data during their work for the Society should receive training and support. They should not be entrusted with personal data unless they can demonstrate their knowledge and competence to handle this information.

Training can be online. Resources are available on the ICO website:

<https://ico.org.uk/for-organisations/sme-web-hub/>

Council Minutes, policy documents, reports and official notices

All Council, Workgroup and Sub-group Minutes and reports are confidential. They sometimes contain sensitive information relating to individuals which cannot be shared in public. Minutes are therefore not published on the web site and are not circulated to the membership in their original form.

Under no circumstances should trustees share Minutes or other confidential documents discussed within the Council, with anyone outside the Council, except with the Council's express permission.

A summary of Council deliberations may be published in the members' Newsletter. Trustee members of the Finance and Governance Group check the newsletter content before publication.

Trustees, non-elected officers and other Society members are not permitted to make unauthorised policy statements on social media.

The Council must approve any new policy statements. Major amendments which constitute a change of policy also require Council approval.

All policy updates must be agreed by all members of the Workgroup concerned. The Workgroups may update existing (previously agreed) policies and make small changes, for example, to contact details, grammar and spelling.

Trustees, non-elected officers and anyone who has previously held one of those positions must never disclose personal data which can identify an individual (names, addresses, and phone or email details) to anyone who does not have an official 'need to know'.

Any trustee or non-elected officer who holds 'old' membership lists (generated more than six weeks previously) must destroy the lists by deletion, confidential shredding or incineration when no longer needed.

All trustees and non-elected officers who hold personal data on paper or digitally have a duty to keep this material safe and not to allow unauthorised access.

Any personal documents or minutes disposed of should be securely shredded or incinerated.

7. Training

The Finance and Governance Group members must keep up to date with training on data protection law and practices. They should encourage staff and trustees to undertake relevant training in order to promote compliance with the UK GDPR;

The Society ensures that all trustees and non-elected officers understand, have access to and can easily interpret the data protection law requirements.

Prospective trustees are informed prior to their application to join the Council that there is a requirement to adhere to our Privacy and Data Protection policies.

8. Document classification and retention

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.

The Society uses a document-labelling protocol when transferring personal data to authorised external parties:

Unrestricted – any document labelled unrestricted, or not labelled at all, is not personal data;

Personal: these documents contain personal data and must be handled according to the UK GDPR;

Strictly confidential – for example, legal disputes and complaints. These documents are handled on a need-to-know basis.

If encryption is used, the secret key is provided to the external party in a separate format.

Public access to the Grassroots database is restricted to members of the Society.

Data is **not encrypted** on transmission to the printers.

Restricted 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 us to obtain, process and share personal information which is only available in a paper format, without anonymisation options, when we process equine passports. Defra, as our regulatory body, acknowledges that these documents can be transferred using standard postal services.

If for any reason a paper copy of personal data must be retained by the Society, we store documents in locked premises.

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. secure shredding, secure incineration, 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.

Document retention times:

Document	Retention time	Disposal
Correspondence	Six months	Secure disposal if personal data included
Complaints	A minimum of seven years. Serious complaints may be retained indefinitely.	Secure disposal
Financial and legal information	Seven years	Secure disposal
Passport information on behalf of Defra	35 years from date of issue ¹ (MOPS para. 18)	Secure disposal if personal data included
Inspection application forms	Seven years (paper/electronic)	Secure disposal
Judges' assessment documents	Seven years	Secure disposal
Equine-related registration and inspection forms	35 years	Secure disposal if personal data included
Council and Sub-Group Minutes	Permanent record in the Minute Book, which is managed by the Company Secretary. Individual trustees should not keep Council minutes beyond	Confidential documents can be sent to the Society's offices for secure destruction.

¹ Where exact copies or scans of paper records, including signatures, are held on electronic record in such a way that they can be easily retrieved and printed for enforcement authorities then there is no need to retain the paper record.

	the end of their term as trustees.	
--	------------------------------------	--

Codes of Conduct and Certification Mechanisms

The Society is a recognised Passport Issuing Organisation (PIO) and as such, is subject to any Codes of Conduct as specified by Defra, the Data Controller.

9. 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 passport-related and membership services, responding to phone calls, printing, DNA analysis and IT systems and services;
- The processing of equine passports and membership applications are currently carried out by Pedigree Livestock Services Ltd under a service level agreement (contract) and data processing agreement. PLS provides telephone response services to members of the public;
- In March 2022, Defra and DAFM agreed rules regarding the processing and updating of equine passports issued by Horse Sport Ireland for horses resident in Great Britain, and vice versa. Currently, naming of horses living in Great Britain which have been imported from Ireland must be carried out by Horse Sport Ireland. Transfers of ownership for Irish-bred horses can be carried out by either PLS or Horse Sport Ireland.
- We monitor and review protocols with Horse Sport Ireland and Defra regarding the processing of equine passports. Passports contain personal data relating to breeders, owners and keepers. Rescinded passports are always returned to the issuing body for secure disposal;
- DNA and associated ownership information is submitted to Weatherby's Scientific in the Republic of Ireland, for DNA parentage-testing;
- We also use Payment Solutions Ltd., trading as SmartDebit, regulated by the Financial Conduct Authority under the Payment Services Regulations 2017;
- Inspection results and some registration information, including breeders' and owners' names and owners' addresses, is submitted to Horse Sport Ireland in the Republic of Ireland, because they are the holders of the Main Studbook for the Irish Draught Horse;
- The names of breeders, owners and keepers of all horses registered or overstamped with the IDHS (GB) are listed on the member-access version of the Grassroots database. This password-protected service is not accessible to non-members. No other contact details are included.
- We may share limited information with other passport-issuing organisations if there is an enquiry that may relate to possible passport fraud. We are obliged to share personal data relating to potential fraud with enforcement agencies (police, Defra, Animal Health, H.M. Revenue and Customs);
- The Society carries out a due diligence exercise, which may include reviewing documents, certifications and references in order to ensure that third party processors have sufficient security measures in place to be effective for the task we are employing them for;
- The Society assesses third-party processors' procedures and activities prior to signing the contract and during the contract period to ensure compliance with the data protection regulations. The Society reviews any codes of conduct under which we are obligated to confirm compliance;

- When choosing a third-party processor, the continued protection of the rights of the Data Subjects is the Society's priority. The Society understands the importance of its continued obligations under the data protection laws, even when a process is handled by a third party;
- A Data Processing Agreement must be completed by both parties and signed as part of the contractual arrangements;
- Processors are notified that they shall not engage another processor (sub-contract) without the Society's prior specific authorisation. Any intended changes concerning the addition or replacement of existing processors must be done in writing, well in advance of any such changes being implemented. Ideally, there should be three clear calendar months written notice of any changes;
- All third-party arrangements are reviewed annually, or when unforeseen circumstances arise.

10. 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 does not have any high-risk processes or processes that could cause impact to a data subject. See Appendix B for the analysis.

The Society will produce DPIA Procedures at the time, should the need arise.

11. Data Subject Rights

Consent and the right to be informed

The Society only processes personal data where there is a legitimate need. Processing personal data is essential for providing services such as membership. Applicants for membership, inspection and passport services are always asked to sign to give their consent to their personal data being processed.

Young people under 18 years of age can sign consent statements provided that a person with parental responsibility countersigns their application. This meets the requirement for data subjects to positively opt-in to having their personal data processed.

Personal Data not obtained from the Data Subject

The Society has no routine processes that require personal data from other sources, but this may be necessary during complaint investigations.

All staff, volunteers and third party processors must be mindful of the requirement not to pass on personal data, for example to put one member in touch with another, without the written permission of the members.

Emails to groups of members, for example with information about judges' assessments, shows or inspections, must be blind-copied to avoid members receiving email addresses for other members.

Subject Access Requests

- The Finance and Governance Group leads on any Subject Access Requests (SARs) from the public and takes action to investigate and report on any breaches of personal data;
- All Subject Access Requests must be sent in writing (or by email) to the Finance and Governance Group, using the group email governance@idhsgb.org.uk
- The Finance and Governance Group will acknowledge any such request within seven working days of receipt;

- The group members will meet to assess any personal data held about the individual and must agree on any redactions necessary. They will, if at all possible, comply with any reasonable request for information. In making the judgement, the following questions should be asked:
 - Is there personal data involved?
 - If there is, does it relate only to the person making the request, or are others mentioned?
 - Who may be harmed if the information is released?
 - Is the information already in the public domain?
 - Has it come from a third party and if so, have they given consent?
- The Society must provide information to the data subject at the earliest convenience, but at a maximum of 28 calendar 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;
- The Data Subject must be 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, for example, because the data originated from a third party, the data subject is informed within 28 days of the reason(s) for the refusal and of their right to lodge a complaint with the Society and/or the Charity Commission or ICO.

Correcting inaccurate or incomplete data

Where inconsistencies are identified and/or where the Data Subject informs the Society that the data held is inaccurate, the Society will take every reasonable step to ensure that such inaccuracies are corrected.

- The Data Subject should write to the Administration Office or to the Finance and Governance Group to request their data be updated;
- The information will be updated as soon as practicable and certainly within 28 days;
- The Society will 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 raise a complaint.

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 either given an erasure date or is monitored so that it can be destroyed when no longer required.
- The Society currently holds an archive of personal data dating back to 1979, when records were kept on paper. The Council has a plan in place to review the personal data held and securely destroy personal data that is no longer required by law.

Automated decision making

The Society does not participate in direct marketing or use automated decision-making processes.

12. Governance and oversight

- The Governance Group has overall responsibility for assessing, testing, reviewing and improving data protection processes, measures and controls in order to identify and mitigate any risks to the protection of personal data and reporting their findings to the Council;
- To this end, the Governance Group will carry out regular audits (at least annually) and compliance monitoring processes to ensure that measures and controls to protect data subjects and their information are adequate, effective and compliant;
- All trustees will be made aware of their individual and collective responsibility for safeguarding personal data;
- Data protection should be a standing agenda item for Council meetings;
- Any improvement plans will be reported to the Council. All reviews, audits and ongoing monitoring processes are available to the Council, the membership, to Defra, the ICO and the Charity Commission if requested.

Data protection and computer security

- Computer systems used on behalf of the Society must be equipped with updated firewall and antivirus protection. This includes any personal computer or other device used by a trustee or non-elected officer who handles personal data as part of their role.
- Any data relating to members of the Society and wider public must be stored in a segregated secure location on the device. Documents containing sensitive material (for example, recruitment information about individuals, complaints) must be encrypted or password-protected.
- Staff, trustees and other volunteers should avoid carrying personal data around on portable media (e.g. flash drives) if possible, as these are easily lost or stolen.
- Computer equipment must be kept in a secure environment. No screens should be within sight of the public at any time.
- Office computer equipment must not be used by anyone other than PLS employees and identified persons providing professional technical support to maintain systems in working order.

Passwords and access codes

- Passwords are a key part of the Society protection strategy. They should be complex and contain at least 8 characters, including letters, numbers and at least one symbol.
- Passwords and access codes must never be recorded on paper and left adjacent to the device, or in unsecured documents on the device.
- No member of staff, trustee or non-elected officer is to give their password or restricted access code to any other person apart from those authorised to provide technical support. Please see the note below regarding password and access code management.

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 Subject” means an individual who is the subject of personal data

“UK GDPR” means the UK General Data Protection Regulation and Data Protection Act 2018.

“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 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 Irish Draught Horse Society (GB), consisting of elected members with the responsibilities of both Directors and Trustees.

Appendix B –Non-Requirement for DPIA Analysis

The factors taken into account were as follows.

- Processing does not involve use of innovative technologies.
- There is no automatic decision-making for access to services.
- No special category data is held.
- There is no profiling of individuals.
- No human biometric or genetic data is held.
- There is no data matching from multiple sources.
- There is no invisible processing, as all personal data comes direct from the data subject.

- There is no tracking of an individual's geolocation or behaviour.
- There is no targeting of children or other vulnerable individuals.
- There is no processing of such a nature that a personal data breach could jeopardise the health or safety of individuals.

Updated by Heather Chaplin, Company Secretary

1 March 2026

Previous versions:

15 January 2009

4 July 2009

3 February 2014

20 May 2018

6 April 2021

20 February 2022, 9 March

26 March 2022

3 December 2022

16 March 2023

8 December 2024

January 2026