Data Protection Policy (version 8)

1. Introduction

The Irish Draught Horse Society of Great Britain (IDHS (GB)) needs to collect 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).*

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 are committed to processing 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.

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, and with Horse Sport Ireland, its parent organisation, both of which are located in the Republic of Ireland. This is required in order to enable equine passports to be issued and processed. Therefore, we are also obliged to adhere to Regulation (EU) 2016/679 of the European Parliament and the Minimum Operating Standards (June 2021) set by Defra.

Data, including titles, names, addresses, telephone numbers, email addresses, dates of birth and membership numbers, is collected from trustees, volunteers, customers, suppliers and members.

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.

3. Consequences of data breaches

The Society has a duty to protect all its members from breaches of privacy and confidentiality. All trustees, staff, volunteers, judges, inspectors, third-party contractors and other officials must adhere to this policy in order to protect the rights of individuals who come into contact with us in the course of our work.

The Society understands that 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.

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.

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

- Fairly and lawfully processed;
- Processed for limited 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 must exercise great care in what records they 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, whether they are a member or not, 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 help.

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

https://ico.org.uk/

5. Governance Procedures

5.1 Establishing compliance

The Society has taken action to meet its data protection obligations and to ensure continued compliance with the regulatory requirements.

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 are checking compliance with data protection legislation and principles.

The Society is working with two other equine passport-issuing organisations, the Dales Pony Society and the British Palomino Society, and with our passport providers, Pedigree Livestock Services (PLS), to ensure that we follow the same principles in terms of data protection in relation to our passport-related services. Please refer to the Data Processing Agreement with PLS for more information.

5.2 Our audit has established that:

- the Society has been registered with the ICO since 30 October 2001. Registration number: Z5960309. The annual fee is payable in advance on 29 October;
- the Society has a Privacy Policy which lists the various types of data that we process. This is published on our web site at www.idhsgb.org.uk;
- data is only processed where the lawfulness of processing has been established;
- we know that data should only be kept 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 timeframes for destruction;
- we are not a public body and do not hold or process personal data falling within the UK GDPR's 'special categories';
- we have checked the current guidelines on the ICO website (13/02/2022) and have confirmed that we are exempt from the requirement to have a named Data Protection Officer;

- the Society has, up until March 2022, relied on one trustee to oversee data protection and carry out due diligence checks on third party organisations. Irrespective of which trustee is responsible, this practice has been identified as a clear potential single point of failure and as such, this arrangement carries avoidable risks.

5.3 Proposed action:

- As part of the planned Council restructuring, we propose that we set up a small team of trustees called 'the data protection team'.
- These trustees are fully accountable to the Council and the membership. The Council will be responsible for significant decisions with a data protection implication.
- The data protection team will act in an advisory capacity to support and advise staff, volunteers and associated third parties with regards to data protection laws and requirements. This will include ensuring that trustees, staff and volunteers who manage and process personal information will be provided with data protection training prior to taking on their roles.
- The data protection team members must be prepared to keep up to date with training on data protection law and practices and be able to assist the Society in monitoring internal compliance with the UK GDPR;
- The team will work together to prepare an action plan for the Council to deal with document retention and secure destruction;
- The team will lead the response to any Subject Access Requests (SARs) from the public;
- The team will keep data minimisation strategies under review and will explore existing and new technologies to ensure that we are protecting data and individuals to the best of our ability;
- The data protection team will ensure that adequate and effective records and management reports are maintained, in accordance with data protection legislation and internal policies.

5.4. Members of the data protection team:

The members of the data protection team will be confirmed during the planned Council restructuring process. As an interim measure, the members are:

- Heather Chaplin 01823 601625 mobile: 07392 299912
- Brian Gates 01461 700434 mobile: 07771 822775
- James Noblett 07909 992274

5.5 Training for compliance

The Society ensures that all staff, trustees and volunteers understand, have access to and can easily interpret the data protection law requirements.

Trustees sign a confidentiality agreement before they take up their posts on the Council. Breaches of Council confidentiality are a disciplinary matter.

Any members of the Society who volunteer to help at inspections or with inspection administration must receive clear instruction regarding their obligations to safeguard any personal data they may see in the course of their work on behalf of the Society. They must also sign a confidentiality agreement regarding their role. This agreement includes a data protection statement regarding the need to keep any personal data confidential.

Trustees and other volunteers are encouraged to undertake training and access support to ensure and demonstrate their knowledge, competence and adequacy for the role.

New and existing staff, trustees and other volunteers will be trained and supported by:

- UK GDPR training sessions
- Individual coaching
- Access to UK GDPR policies, procedures, and supporting documents.

Some training resources are available on the ICO website:

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

5.6 Principles for procedures

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.

5.7 Some personal data is included in our publications and/or electronic forms:

- Lists of staff, judges, trustees and candidates for judges' assessment and inspection-related training days
- the publication of foals registered each year (breeders' names)
- lists of stallions that are the subject of inspection applications or which have been inspected, and those standing at stud (owners' names and full contact details)
- lists of mares that are the subject of inspection applications or which have been inspected (owners' names)
- lists of inspected animals that are submitted to Horse Sport Ireland (this data is sent to the EU) - mare owners' names and stallion owners' full contact details
- lists of mares that have received a Hornby Premium (owners' names)
- Show catalogues produced for general public information (members' names)
- on the members' access Grassroots database (names only - breeders, owners and keepers)
- Emails received from, or sent to, members of the public and trustees.

5.8 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 filing cabinets 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 incinceration, 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.

5.9 Data storage times:

- Correspondence: six months, unless there are legal or contractual implications – secure disposal required.
- Financial and legal information: seven years – secure disposal required.
- Passport information on behalf of Defra: 35 years, as specified in the Minimum Operating Standards (MOPS, para 18) – secure disposal if personal data is included. '(The) PIO must keep records for at least 35 years or until at least 2 years from the date of death of the animal concerned, as required by the retained 2016 Regulation (for England and Wales) or the 2016 EU Regulation (for Northern Ireland) Article 38(2). 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.'
- Inspection information relating to owners and agents: up to seven years - – secure disposal is required.
- Council Minutes: there is a permanent record in the Minute Book, which is managed by the Company Secretary and the Administrator. Individual trustees should not keep Council minutes beyond the end of their term as trustees.

5.10 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.

5.11 Third-Party Processors: due diligence

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.

5.12 Third party arrangements:

- 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 may also provide telephone response services to members of the public;
- From March 2022, equine passports issued by Horse Sport Ireland for horses resident in Great Britain must be processed by Pedigree Livestock Services. This is a Defra requirement, as specified in the Minimum Operating Standards (June 2021). We establish and review protocols with Horse Sport Ireland and Defra regarding the processing of these passports, which contain personal data relating to breeders, owners and keepers.
- 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 equine (non-personal) information with other passport-issuing organisations if there is an enquiry that may relate to possible passport fraud. We only 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 should be reviewed at agreed intervals, for example, after six months and thereafter annually, or when unforeseen circumstances arise.

6 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.

7 Data Subject Rights Procedures

7.1 Consent and the right to be informed

The collection of personal data is a fundamental part of the services offered by the Society. We only process personal data where there is a legitimate need.

Processing personal data is essential for providing services such as membership. The personal data required is a precondition of a service we are offering. 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.

The Society uses the Grassroots 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.

Members of the Society have access, through a user name and password, to Grassroots to enable them to look up individual horses in the breeding herd and Sport Horse Register. The only personal data that members can see is the name of the animal's breeder, keeper and owner.

Addresses and other contact information are not visible to members on the Grassroots system.

Confidential information about a horse, for example, alerts about ownership disputes or veterinary findings, must never be placed in the 'Description' field, which is visible to members.

7.2 Information Provisions

The Society provides a separate 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 obtain further information. Individuals are referred to the Privacy Statement at the time we collect their personal data (or at the earliest opportunity, when that data is obtained indirectly).

7.3 Personal Data not obtained from the Data Subject

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

7.4 Subject Access Request

- Subject Access Requests (SAR) are passed to the Society's Administrator as soon as received;
- The Administrator records the request and passes it to the data protection team, as well as the Society's Chair, Company Secretary and Vice Chair not more than 48 hours after receipt;
- The request must be acknowledged within seven working days of receipt;
- The team checks the personal data held about the individual to see who else it has been shared with and any specific timeframes for access. The team should agree on what personal data, if any, needs to be redacted;
- The Society must provide information to the data subject at the earliest convenience, but at a maximum of 28 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.

7.5 Trustee, volunteer and customer personal data

Personal data is collected for the following reasons:

The Society's policy is that all trustees and volunteers have to be members of the Society. Membership requires personal data to be collected.

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.

Some owners submit inspection application forms or expressions of interest, including their contact details, before they have joined the Society.

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.

7.6 Correcting inaccurate or incomplete data

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

- The Administrator 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 28 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 ICO and to a judicial remedy.

7.7 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 required.

The Society currently holds an archive of personal data dating back to 1979, when records were largely kept on paper. The Data Protection Team will propose a plan to put to the Council to review the personal data held and securely destroy personal data that is no longer required by law.

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, which have to be kept for 35 years.

The Society may carry out research for which membership lists are required. These are destroyed when no longer needed.

7.8 The right to restrict processing

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

7.9 Objections and automated decision making

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

8 Oversight Procedures

8.1 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.

8.2 Trustees and volunteers - security arrangements

Trustees, staff and volunteers 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'. For example, any trustee who holds 'old' membership lists (generated more than four weeks ago) must destroy the lists by confidential shredding or incineration when no longer needed.

All trustees and volunteers have a duty to keep personal data in a safe place within their homes and not to allow unauthorised access. Any personal documents or minutes disposed of should be securely shredded or incinerated

8.3 Data protection and computer security

- IDHS (GB) computer systems must be equipped with updated firewall and antivirus protection, as must any personal computer used by a trustee or other volunteer 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 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 authorised trustees, employees of the Society and identified persons providing professional technical support to maintain systems in working order.
- No member of staff or trustee is to give their password or restricted access code to any other person apart from those providing technical support. Please see the note below regarding password and access code management.
- Any breach of confidentiality, including data loss, whether accidental or through unlawful activity such as hacking, must be reported to the Data Protection Team immediately.

8.3.1 Passwords and access codes

- Passwords are a key part of the Society protection strategy and are used throughout the Society to secure information and restrict access to systems. Passwords must be complex and contain at least 8 characters long, 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.
- Passwords and restricted access codes are strictly confidential and must never be shared with a third party. If they have to be given to a person who is carrying out repair work on computer hardware or re-installing software, this person must be supervised at all times while the work is carried out. The password must be changed immediately once the work is completed.

8.4 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.

Horse owners can choose to pay extra to have their horse's passport mailed by Special Delivery or 'signed for'.

With the exception of regulators and enforcement agencies, horse owners' personal information can only be shared when prior written permission has been given.

All the Society's forms were updated when the UK General Data Protection Regulation came into force in May 2018 and were updated again in April and December 2021. In addition to the existing data protection safeguards from the 1984 and 1998 Acts, individuals have to positively 'opt in' to permitting the Society to hold personal data on them.

The wording on our forms and application documents has been amended to reflect this and must not under any circumstances be removed from those documents, unless a change to the wording is required by subsequent legislation.

If in any doubt about whether to disclose information, staff and trustees must seek advice from the data protection team or the ICO.

9. Data protection monitoring

This policy documents 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 codes of conduct. These measures include:

- the data protection team 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 data protection team 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 and to the ICO if requested.

10. How trustees can request access to personal data for research or providing a service to members

Any member of staff or trustee who wishes to access personal data, for example to complete a specific project which requires them to contact members, must discuss their request with the data protection team in the first instance.

The Council should be informed of, and approve, such requests.

The person or group carrying out the research should update their knowledge of the data protection policy and current legislation before embarking on the project.

11. Legal obligations to share personal data with enforcement agencies

Enforcement agencies, such as Defra, the police, Animal Health officials from the Trading Standards department and H.M. Revenue and Customs may instruct us to share personal data held in our records with them. This is mandatory in the context of prevention or detection of crime or animal disease tracing.

The Society will cooperate with identified officials from these regulatory bodies at all times. Failure to do so would be obstruction.

12. Public access to Council minutes

Council agreed that a summary of each Council meeting, with the main action points, should be placed on our web site as soon as the content has been approved by the Council. These summaries should also be published in the news sheets. They will not contain sensitive or third-party information.

Council Minutes that identify an individual can be requested by that person through the provisions of a Subject Access Request under the Data Protection legislation. In order to access their own personal data held by the Society, the applicant should write to the data protection team c/o the Administrator, who will follow the procedure outlined in paragraph 7.4 above (Subject Access Requests).

The Society should, 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?

We have a legal duty to provide this information to the individual concerned. When the Minute relates only to the person making the request, we have no option but to release it to them. If that person points out a factual inaccuracy, it must be amended immediately.

Minutes must be redacted to remove third party information before releasing them either onto the web site or to a person making a request for access.

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

Drafted by Heather Chaplin, Trustee

Versions:

15 January 2009
4 July 2009
3 February 2014
20 May 2018
6 April 2021

20 February 2022, 9 March
26 March 2022 (this version).

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.