



CONQUEST
CENTRE

Conquest Farm, Norton Fitzwarren
Taunton, Somerset. TA2 6PN
01823 433614
info@conquestcentre.org.uk

Conquest Centre

Data Protection Policy

Policy Owner	Data protection Officer
Date of Original Issue	08.2021
Policy Last Reviewed	01.2026
Date of Next Review	01.2027
Version	V1


Animals • Wellbeing • Nature • Connection

DATA PROTECTION POLICY

Table of Contents

	Page
1. Data Protection Origins	3
2. Conquest Data Protection Policy Overview	4
3. Conquest's Commitment	4
4. Processing Personal Data	5
5. Personal Data Management	7
6. Data Subject Access	8
7. Data Protection Officer	9
8. Data Protection Measures	9
9. Conquest Data processes	10
10. Data Breaches	11
11. Fundraising	11
12. Managing Financial Data	12
13. Beneficiary Data	12
14. Policy Review	13
Appendix	
A Data Consent.	14
B Subject Access Request Form	16
C Privacy Impact Statement	17
D Data Breach Checklist and Assessment Form	18
E Data Breach Reporting Form	20
F Data Breach Register	22

DATA PROTECTION POLICY

1. Data Protection Origins

1.1. The European Union's data protection laws are regarded as a leading standard all over the world. The UK was covered by the Data Protection Act 1998 (DPA) which came into force on the 1st March 2000. That Act came from the 1995 European Data Protection Directive; part of the EU's body of privacy and human rights law. The DPA and the European Data Protection Directive regulated the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

1.2. Since the introduction of the DPA in 1998, technology, and how it is used to process data, has radically transformed the way organisations operate. To adapt to modern technology, in 2016, the EU adopted the General Data Protection Regulation (GDPR). It replaces the 1995 Data Protection Directive and came into effect on 25 May 2018.

1.3. The GDPR is employed across the EU and Member States and incorporated within the UK's government Data Protection Bill. The act:

1.3.1. • Reflects modern, digital practices for handling data. The Bill also allows the Information Commissioners Office (ICO) power to bring criminal proceedings against offences of malpractice;

1.3.2. • Contains local derogations allowed by GDPR as seen in UK Law;

1.3.3. • Introduces two offences within the UK, the:

1.3.3.1. • 'Re-identification of de-identified personal data' - the matching of de-identified data with publicly available information in order to identify the individual to which the data belongs to;

1.3.3.2. • 'Alteration of personal data to prevent disclosure' - this offence criminalises the alteration of personal data after a subject access request has been filed with a data controller.

1.4. Data Protection Bill can be found at www.gov.uk/guidance/data-protection-bill-overview

1.5. In the UK, the GDPR will be overseen by the ICO. The ICO is an independent public body set up to uphold information rights in the public interest. The ICO sit independently of government, though are sponsored by the Department for Digital, Culture, Media and Sport (DCMS). The ICO will have powers to take action where organisations are failing to comply with the law; as indeed the ICO do currently with the existing Data Protection laws. The ICO

also has powers under the Privacy and Electronic Communications Regulation (PECR) which governs the use of electronic means of marketing such as emails, text messages, etc., which was updated in 2016.

1.6. Personal Data is simply identified as 'Personal' if it is concerned with identifiable living individuals, irrespective of the data being processed automatically, electronically or manually; and recorded 'Data' (not unrecorded conversations with service users, donors or customers).

1.7. GDPR defines 'Personal Data' as - any information relating to an individual or identifiable natural person (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, an online identifier, or to one or more of the factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person). For data to be classified as sensitive personal data it must fall into the following categories:

- 1.7.1. • The racial or ethnic origin of the subject
- 1.7.2. • The subject's political opinions
- 1.7.3. • The subject's religious beliefs or beliefs of a similar nature
- 1.7.4. • Whether the subject is a member of a trade union
- 1.7.5. • Information on the subject's physical or mental health condition
- 1.7.6. • Information on the subject's sexual life
- 1.7.7. • The commission or alleged commission of an offence by the data subject
- 1.7.8. • Information relating to the commission or alleged commission of an offence by the data subject. The Special Categories now specifically includes Biometric Data and Genetic Data where processed to uniquely identify an individual. (e.g., fingerprint payment systems).

1.8. Valid reasons for processing the data are:

- 1.8.1. • The individual whom the personal data is about has consented to the processing;
- 1.8.2. • The processing is necessary: in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract;

- 1.8.3. • The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract);
- 1.8.4. • The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident;
- 1.8.5. • The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions;
- 1.8.6. • The processing is in accordance with the "legitimate interests" condition.

2. Conquest Data Protection Policy Overview

2.1. Compliance with the GDPR is a legal requirement and is to be followed at all times by Conquest Equestrian Centre (NB: Charity - 'Conquest Centre Ltd' and Business - 'Conquest Equestrian Centre Ltd'. Both hereafter known as 'Conquest'), its staff, volunteers, contractors, trustees, sponsors or other parties working on behalf of Conquest (hereafter known as 'Data Processors'). This Policy sets out the obligations of Conquest regarding the protection of personal data and the rights of staff, trustees, clients, volunteers, sponsors, donors, customers, suppliers, and partners (hereafter known as 'Data Subjects'). This Policy does not form part of an employee's contract of employment and may be amended at any time. Conquest places high importance on the correct, lawful, and fair handling of all personal data respecting the legal rights, privacy and trust of all individuals with whom it deals.

2.1.1. • The scope of Conquest's Data Protection Policy covers the following information:

- 2.1.1.1. • What data Conquest keeps and why it keeps this data
- 2.1.1.2. • To what types of data the policy applies
- 2.1.1.3. • Identify who at Conquest is responsible for processing the data
- 2.1.1.4. • The main data risks faced by Conquest
- 2.1.1.5. • Key precautions to keep data protected
- 2.1.1.6. • How data should be stored and backed up
- 2.1.1.7. • How Conquest ensures data is kept accurate and when data will be deleted
- 2.1.1.8. • What to do if an individual asks to see their data and when Conquest will turn down a Subject Access Request
- 2.1.1.9. • Under what circumstances Conquest discloses data, and to whom

- 2.1.1.10. • How Conquest keeps individuals informed about data it holds
- 2.1.1.11. • The role of Conquest's Data Protection Officer
- 2.1.1.12. • Who is responsible for reporting any breaches to the ICO and Charity Commission

3. Conquest's Commitment

3.1.

Conquest agree that all confidential and personal identifiable information concerning the staff, clients, volunteers, customers, suppliers and partners (hereafter known as 'Personal Data') will be held securely and in confidence using appropriate technical and organisational measures. Conquest is committed to compliance with General Data Protection Regulation (EU) 2016/679 (hereafter called 'GDPR') and relevant UK and EU data protection legislation in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Conquest collects and processes. Specifically, Personal Data:

3.1.1. • Must be processed lawfully, fairly and in a transparent manner in relation to individuals' rights

3.1.2.

- Shall be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not be considered to be compatible with the initial purposes

3.1.3. • Must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed

3.1.4.

- Has to be accurate and kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which that are processed is erased or rectified without delay

3.1.5.

- Must be kept in a form which permits identification of all persons associated with Conquest for no longer than is necessary for the purposes for which the personal data is processed. Personal data will be deleted after a set period if the Data Subject has had no data activity over a set period of time - with the exception of

Data Subject Deleted Data if Inactive for (yrs)

Staff	7
Trustee	3
Client	1
Volunteer	1
Sponsor	10
Donor	10
Customer	1
Supplier	7
Partner	3

3.1.6. Storage of personal data may be stored for longer periods in the interests of accident/incident recording subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the Data Subject;

3.1.7. Is to be processed ensuring appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Processing Personal Data

4.1.

Conquest collects and processes Personal Data (Reference - <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>) directly from Data Subjects and/or from third parties and will only process the Data for the specific purposes set out in this Policy. GDPR identifies that the Data Subject has the right to:

- 4.1.1. • Be informed
- 4.1.2. • Have access to their data
- 4.1.3. • Reflect on the data provided
- 4.1.4. • Have data erased (also known as the 'right to be forgotten')

- 4.1.5. • Restrict their data being processed
- 4.1.6. • Data portability
- 4.1.7. • Object and have their data used for automated decision-making or profiling

4.2. The purposes for which Conquest processes Personal Data will be communicated to the Data Subject at the time of their Personal Data collection, where it is collected directly from them, or as soon as possible after Data is collected from a third party. Conquest will:

4.2.1. • Process Personal Data during the term of the Agreement, unless otherwise agreed by the Data Subjects and will be a Data Processor in accordance with the GDPR

4.2.2. • Only act on the written instructions of the Data Subjects (unless required by law to act without such instructions)

4.2.3. • Process personal data on behalf of the Data Subjects to fulfil the contract obligations to provide pre-employment screening services on their behalf

4.2.4. • Only screen the Data Subjects to the screening level agreed to and ordered by the individual concerned

4.2.5. • Process personal identifiable information under instruction from the Data Subjects. The information collected about the data subject will be limited to what is necessary to fulfil the Data Subjects involvement with Conquest. The information may include:

- 4.2.5.1. • Name/previous names
- 4.2.5.2. • Current address/previous addresses
- 4.2.5.3. • Date of birth - age - gender
- 4.2.5.4. • Medical information
- 4.2.5.5. • Criminal record
- 4.2.5.6. • Qualifications, institutes of study, personal and professional references
- 4.2.5.7. • Current and past employments
- 4.2.5.8. • Identification documents

4.2.6.

• Ensure any access by partners or third parties working with Conquest will be subject to the same conditions and must provide the same level of protection for the fundamental rights of the data subject;

4.2.7. • Hold Personal Data securely in the UK;

4.2.8.

• Not sell Personal Data to third parties, nor copy or disclose Data to any third-party other than those required to conduct the service entered into by the organisation;

4.2.9.

• Recognise Data Subjects at Conquest as Data Controllers in their own right. Therefore, when processing Personal Data, a Data Controller is obligated to comply with the GDPR.

4.2.10. • Seek to make the following information available to the Data Subject:

4.2.10.1. • Details of Conquest and name of the Data Protection Officer;

4.2.10.2.

• The purpose of the Personal Data being collected - if required, the legal basis and legitimate interests justifying the data collection;

4.2.10.3.

• Where Personal Data is not obtained directly from the Data Subject, the scope of the Personal Data collected and processed;

4.2.10.4. • Where Personal Data has been transferred to one or more third party, details of those parties;

4.2.10.5. • Details of the length of time the Personal Data will be held by Conquest;

4.2.10.6. • Details of the Data Subjects rights under GDPR;

4.2.10.7. • Details of the Data Subject's rights to withdraw their consent to Conquest's processing of their Personal Data at any time;

4.2.10.8. • Details of the Data Subject's right to complain to the ICO;

4.2.10.9.

• Details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it;

4.2.10.10.

• Details if any automated decision-making that will take place using the Personal Data, including information on how decisions will be made, the significance of those decisions and any consequences.

4.2.11. • Not transfer Personal Data outside of the European Economic Area (EEA) without the explicit consent from the Data Subject and only after they have been informed of the possible risks of such transfer. Data transferral will only be done outside the UK if there is an appropriate “level of protection for the fundamental rights of the data subjects” For this to happen specified safeguards apply including EU acceptance of adequacy, membership to Privacy Shield, acceptance of model contract clauses, binding corporate rules or the assessment of adequacy by Conquest.

5. Personal Data Management

5.1. Personal information about the Data Subjects will be held by Conquest for the duration of their association with Conquest. After this period the information will be deleted so that it is beyond use with the exception of specific data that refers to incidents and accidents. That data will contain the minimum amount of information required as reference information required for future legal and medical claims. Conquest takes appropriate organisational and technical measures to ensure the security, data protection and privacy of data processed by Conquest on behalf of the Data Subjects. This includes alignment to ISO27001, ISO22301, BS10012, ISO9001, ISO14001 and Cyber Essentials. All reasonable steps are taken to protect Personal Data against unauthorised, unlawful processing and against accidental loss, destruction or damage. Personal Data consent will be given by each data subject; they will be provided with details of how to access Conquest's Data Protection Policy and/or, in the case of Volunteers, Students, Clients, Donors and Sponsors, asked to agree with the Conquest's Data Protection Policy statement (Appendix A - Data Consent).

5.2. Conquest will ensure that Data Processors will comply with GDPRs. GDPR seeks to ensure that personal data is processed lawfully, fairly and transparently without adversely affecting the rights of the data subject. GDPR requires the processing of data if at least one of the following applies:

5.2.1. • The Data Subjects have given consent to the processing of his or her personal data for one or more specific purposes;

5.2.2. • Processing is necessary for the performance of a contract to which Data Subjects is a party or in order to take steps at the request of the data subject prior to entering a contract;

5.2.3. • Processing is necessary for the compliance with a legal obligation to which Conquest is subject;

5.2.4. • Processing is necessary to protect the vital interests of the data subject or of another natural person;

5.2.5. • Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Conquest;

5.2.6. • Processing is necessary for the purpose of the legitimate interests pursued by Conquest or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

5.3. All Personal Data will be kept accurate and up to date. The accuracy of the Personal Data will be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date Personal Data is found, all reasonable steps will be taken to amend or erase that Personal Data as appropriate. Personal Data inaccuracies will be amended within one month and the Data Subject informed of its completion.

5.4. Data Portability. Where Data Subjects have given their consent to Conquest for the processing of their Personal Data in such a manner or the processing is otherwise required for the performance of a contract between Conquest and the Data Subject, Data Subjects have the legal right under GDPR to receive a copy of their Personal Data and to use it for other purposes.

5.6. To facilitate the right of data portability, Conquest will make available all applicably Personal Data to Data Subjects and, where technically feasible and if requested by the Data Subject, Personal Data will be sent directly to another Data Controller.

5.7. Data Subjects have the right to object to Conquest processing their Personal Data based on legitimate interests, advertising, direct marketing including profiling and statistical purposes. Where a Data Subject objects to Conquest processing their Personal Data:

5.7.1. • On legitimate interests, Conquest will cease such processing forthwith, unless it can be demonstrated that Conquest's legitimate grounds for such processing over-rides the Data Subject's interests, rights and freedoms, or the processing is necessary for the conduct of legal claims;

5.7.2. • For direct marketing purposes, Conquest will cease such processing forthwith;

5.7.3. • For statistical purposes, the Data Subject must, under GDPR, demonstrate grounds relating to their particular situation. Conquest is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

5.8. Profiling is used by Conquest to evaluate certain personal aspects of an individual i.e., to analyse the performance at work, health, personal preferences, reliability, movement etc and provide information to Donors and funders/supporters. Where Conquest uses Personal Data for profiling purposes, the following will apply:

- 5.8.1. • Clear information will be provided to the Data Subject explaining the profiling, including its significance and likely consequences;
- 5.8.2. • Appropriate and mathematical or statistical procedures will be used;
- 5.8.3. • Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected will be implemented;
- 5.8.4. • All Personal Data will be secured in order to prevent discrimination effects arising out of profiling.

5.9. If requested by the Data Subjects, Conquest shall permanently destroy all confidential information held in its possession or under its control except for specific data that refers to incidents and accidents. That data will contain the minimum amount of information required as reference information required for future legal and/or medical claims.

6. Data Subject Access

6.1. Conquest shall assist a Data Subject in providing subject access requests (SAR) using Conquest's 'Subject Access Request Form' (at Appendix B) and allowing data subjects to exercise their rights under the GDPR. SARs will:

- 6.1.1. • Be forwarded to the Data Protection Officer or the Conquest Manager within 24 hours of receipt;
- 6.1.2. • Be assessed for viability and should it be deemed manifestly unfounded, excessive or adversely affect the rights and freedoms of others, Conquest will refuse the request;
- 6.1.3. • Not draw down a financial fee; however, Conquest reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

6.2. Conquest shall assist Data Subjects with audits and inspections, providing them with information they need to ensure that Conquest and the individuals are meeting their obligations under GDPR Article 28. In addition, Conquest will inform Data Subjects if Conquest are asked to do something infringing the GDPR or other UK, EU or member state data protection law.

6.3. Conquest will assist the Data Subject, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

6.4. Conquest will co-operate with supervisory authorities (such as the Information Commissioner's Office (ICO)) in accordance with GDPR Article 31 and will keep records of its processing activities in accordance with GDPR Article 30.2.

6.5. Conquest will notify any personal data breaches to Data Subjects in accordance with GDPR Article 33

6.6. Conquest employs a data protection officer as required by GDPR Article 37.

6.7. Data Subjects are to acknowledge that Conquest is reliant on them for direction as to the extent to which Conquest is entitled to use and process their Personal Data. Consequently, Conquest will not be liable for any claim arising from any act or omission by Conquest, to the extent that such act or omission resulted directly from the Data Subjects instructions.

7. Data Protection Officer

7.1. The UK mandates a requirement to appoint a Data Protection Officer (DPO) in certain situations. Conquest's DPO is created because Conquest:

- 7.1.1. • Is a Charitable organisation;
- 7.1.2. • Processes data activities which involve regular monitoring of data subjects covering a large range of data topics;
- 7.1.3. • Employs a core activity processing sensitive personal data.

7.2. The Conquest DPO will keep written internal records of all Personal Data collection, holding and processing methods. They are accountable for the following information:

- 7.2.1. • The recording of Conquest's DPO and any third-party data controllers;
- 7.2.2. • The purposes for which Conquest processed Personal Data;
- 7.2.3. • Details of the scope of Personal Data collected, held and processed by Conquest and how the Personal Data relates to the Data Subject;
- 7.2.4. • Details of any third parties that will receive Personal Data from Conquest and on what basis. A copy of any agreement requesting the transfer Personal Data must be kept

and reviewed prior to signing to ensure processing provisions are compliant with GDPR. The DPO is to be integrally involved in all Conquest contract negotiations;

7.2.5. • Details of how long Personal Data will be retained by Conquest;

7.2.6. • Detailed descriptions of all technical and organisational measures taken by Conquest to ensure the safety of Personal Data.

7.3. Conquest will undertake a Privacy Impact Statement (at Appendix C) on Personal Data and overseen by the DPO. The DPO will address the following:

7.3.1. • The purpose(s) for which Personal Data is being processed and the processing operations to be carried out on that Personal Data;

7.3.2. • Details of the legitimate interests being pursued by Conquest;

7.3.3. • An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

7.3.4. • An assessment of the risks posed to individual Data Subjects;

7.3.5. • Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of Personal Data, sufficient to demonstrate compliance with GDPR.

8. Data Protection Measures

8.1. Conquest Information Systems - Acceptable Use Policy. Data Processors will maintain IT security by protecting the confidentiality, integrity and availability of Personal Data as defined in Conquest's IT Policy. All Conquest Data Processors shall comply with the following when working with Personal Data:

8.1.1. • All Conquest Data Processors must use their issued Conquest 365 email address for all work involving Personal Data. The use of personal email addresses for this purpose is strictly forbidden;

8.1.2. • Where any Personal Data is to be erased or disposed of it should be done securely. Hardcopies are to be shredded and electronic copies are to be deleted securely using the procedures detailed in the IT Policy

8.1.3. • Transmission of Personal Data should use secure networks only;

8.1.4. • Personal Data contained in an email should be stored securely and the email, and any temporary files associated with the email, is to be deleted;

8.1.5. • Where Personal Data is sent by facsimile transmission, recipients are to be informed in advance and be awaiting the receipt of the Personal Data at the point of delivery;

- 8.1.6. • Hardcopy Personal Data should be passed directly to the recipient;
- 8.1.7. • Disclosure of Personal Data may be shared with any member of Conquest providing there is a legitimate need to do so;
- 8.1.8. • No Personal Data may be shared to other parties without the authorisation of the Conquest Manager and/or the DPO;
- 8.1.9. • All hardcopies of Personal Data, along with electronic copies stored on removable media, should be stored securely in a suitable lockable container;
- 8.1.10. • Personal Data must be handled with care at all times and should not be left unattended or on view by unauthorised persons;
- 8.1.11. • Personal Data users must ensure that individual monitors do not show confidential information to others and that they log off from their PC, or other device, when it is left unattended;
- 8.1.12.
 - If using a laptop, tablet computer, memory stick, smartphone, other mobile device or an approved personal device, Data Processors must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on any equipment to protect confidential data in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport. NB: Personal data regarding individuals should only be removed from the office on portable devices where it has been encrypted so that it is protected if that device is lost or stolen;
- 8.1.13.
 - All Personal Data process and stored electronically will use accredited software, password protected and will be backed up - as detailed in the Conquest IT policy;
- 8.1.14.
 - All passwords protecting Personal Data should be changed regularly - passwords are to contain a combination of uppercase and lowercase letters, numbers and symbols. Passwords are not to be recorded and, if forgotten or changed, reset by approved methods as detailed in the Conquest IT Policy;
- 8.1.15.
 - Updates to Conquest PCs and devices are applied as required by the IT Manager. Privately owned devices used for Conquest work must be regularly updated by the owner;
- 8.1.16.
 - Downloads or the installation of software on to Conquest systems from external sources are not permitted without the authorisation of the IT Manager.

8.1.17.

- Data collection techniques including 'cookies' should be revised to ensure that excessive data collection is not occurring and that automated deletion processes are in place to remove Personal Data after a set period of time.

9. Conquest Data processes

9.1. Conquest is to ensure the following measures are taken with respect to the collection, holding and processing of Personal Data:

- 9.1.1. • Data Processors are to be made aware of their individual responsibilities Conquest's Data Protection and are to comply with the Policy at all times;
- 9.1.2. • Personal Data will only be accessed by Conquest Data Processors in order to carry out their duties;
- 9.1.3. • Data Processors will receive training and advice as to how to handle Personal Data;
- 9.1.4. • Personal Data used by external bodies will be appropriately supervised, authorised and are to follow GDPR principles;
- 9.1.5. • Data processing will be regularly monitored, audited and reviewed.
- 9.1.6. • Data Processors will be evaluated and reviewed regularly.

10. Data Breaches

10.1. A personal data breach is defined as “a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.” If Conquest has a personal data breach, the Data Breach Checklist and Assessment Form (Appendix D) is to be enacted which will:

- 10.1.1. • Investigate the data breach and perform an initial assessment as to the severity of the incident;
- 10.1.2. • Notify internally and, if necessary, identify who to notify externally. Conquest is to ensure that a robust breach detection, investigation and internal reporting procedures are in place. Following ICO's guidance, both the Regulator/Supervisory Authority and Data Subject will be notified within 72 hours of the data breach using Conquest's 'Data Breach Reporting Form' (Appendix E) and recorded on the Data Breach Register (Appendix F). Further reference to the latest ICO reporting policy can be found at: www.ico.org.uk/for-organisations/report-a-breach/.

10.2. Along with reporting a data breach to the ICO, Conquest will also need to consider whether the data breach is a serious incident, and if so whether to report to the Charity Commission - further direction can be found at <https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity>. Data breaches are classed serious when:

- 10.2.1. • Conquest's data has been accessed by an unknown person; this data was accessed and deleted, including the charity's email account, donor names and addresses;
- 10.2.2. • A Conquest laptop, containing personal details of beneficiaries or staff, has been stolen or gone missing and it's been reported to the police;
- 10.2.3. • Conquest funds lost due to an online or telephone 'phishing scam', where trustees were conned into giving out bank account details;
- 10.2.4. • A Data Protection Act breach has occurred and been reported to the ICO.

10.3. Data breach notifications will include:

- 10.3.1. • Categories and number of Data Subjects concerned;
- 10.3.2. • Types and number of Personal Data records concerned;
- 10.3.3. • Contact details of Conquest DPO;
- 10.3.4. • Likely consequences of the data breach;
- 10.3.5. • Identification of the measures taken to address the breach and what has been done to mitigate its possible diverse effects.

11. Fundraising

11.1. Conquest primarily operates an income generation scheme using donors, sponsorship and fundraising (hereafter known as 'Funders'). The minimum amount of Personal Data of Funders is retained by Conquest, it is stored securely and processed only by those Data Processors authorised as part of their job description to do so. Conquest will not pass on Funders Personal Data to third parties.

11.2. Collection of Funders Personal Data will clearly identify the:

- 11.2.1. • Funders consent - consent must be unambiguous, freely given, demonstrable, specific and informed;
- 11.2.2. • Justification for the need of financial contributions;
- 11.2.3. • Opt-in, opt-out options;

- 11.2.4. • Funders rights are protected, and information is available as to:
 - 11.2.4.1. • Why Personal Data is collected;
 - 11.2.4.2. • What is done with the Personal Data;
 - 11.2.4.3. • How Personal Data is shared - if at all;
 - 11.2.4.4. • How Personal Data is stored;
 - 11.2.4.5. • When Data Subjects can access their Personal Data.
- 11.2.5. • Personal Data retention duration;
- 11.2.6. • Personal Data disposal instructions.

11.3. Personal Data will be retained by Conquest for six years to satisfy Gift Aid and HMRC requirements, but other Personal Data may be retained indefinitely depending on the Funders background and potential for continuing financial support of Conquest. Funders Personal Data will be monitored regularly. Information on Fundraising can be found at: <http://bit.ly/IOFGDPR>.

12. Managing Financial Data

12.1. Financial data of Data Subjects are held securely by Conquest and is accessed only by authorised Conquest Data Processors. Financial Personal Data records are kept manually and electronically and cover:

- 12.1.1. • Conquest staff records, including salary, tax and pension records;
- 12.1.2. • Volunteer Personal Data (as required);
- 12.1.3. • Client Personal Data including financial records;
- 12.1.4. • Supporter and Funders data including donations, support provided and any additional financial linked data i.e., copies of cheques, bank details, property, livery and equipment purchases;
- 12.1.5. • Suppliers' information, including email addresses or contact information of those that are providing goods or services to Conquest - including bank details;

- 12.1.6. • Beneficiary financial data, such as grants made or financial assessments.

12.2. Personal Financial Data will be retained by Conquest for a period of 7 years (tax purposes). Data Subjects have rights to complain (4.2.10.8), maintain their individual rights (2.1.1) and are able to initiate a SAR (6.1); additionally, detailed information about bank details will be reviewed annually and any financial data no longer relevant will be deleted. Data Subjects Financial Data is to be used for legitimate purposes only.

12.3. Conquest's financial controller will use Personal Data to generate reports, track their production, disseminate the reports according to their usage and use assured disposal processes when the financial reports are no longer required.

13. Beneficiary Data

13.1. Client/beneficiary Personal Data held by Conquest, both manual and electronic, needs to be clearly identified and understood. Consent must be agreed and recorded before any Personal Data is obtained. The beneficiary must understand:

13.1.1. • What Personal Data is held, including the duration of time that they are to be held. Beneficiaries consent must be specific, informed, withdrawn and at any time, freely given, involve clear affirmative action and be verifiable;

13.1.2.

- The location and types of Personal Data held and what work has been undertaken to obtain and cleanse the records;

13.1.3. • That Personal Data held may constitute sensitive data, especially in relation to Personal Data relating to children and medical conditions;

13.1.4. • The process by which the Personal Data has been obtained, including, whether there is a duplicate between electronic and locally held records;

13.1.5.

- The implications of providing financial data such as grants, financial assessments and/or salary records;

13.1.6. • The individuals responsible for the Personal Data at each stage of the process.

13.2. Personal Data of beneficiaries may be obtained through a variety of methods in order to increase Conquest's performance and effectiveness. Whichever method is used in the

acquisition of Personal Data consent is to be achieved, they retain their right to complain (4.2.10.8), the maintain their individual rights (2.1.1) and their ability to initiate a SAR (6.1).

13.3. Under GDPR Article 8(2), Conquest will need to make 'reasonable efforts' to verify that consent has been given or authorised for the collation of children's Personal Data from their parent, guardian, carer or 'the holder of parental responsibility' except when Conquest needs to process children's Personal Data in relation to preventative or council services that directly affect the child.

14. Policy Review

14.1 The Data Protection Officer is responsible for monitoring and reviewing this policy. This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or government advice may trigger interim reviews.

Appendix:

- A Data Consent.
- B Subject Access Request Form.
- C Privacy Impact Statement.
- D Data Breach Checklist and Assessment Form.
- E Data Breach Reporting Form.
- F Data Breach Register

1. Data Protection Origins

- 1.1. The European Union's data protection laws are regarded as a leading standard all over the world. The UK was covered by the Data Protection Act 1998 (DPA) which came into force on the 1st March 2000. That Act came from the 1995 European Data Protection Directive; part of the EU's body of privacy and human rights law. The DPA and the European Data Protection Directive regulated the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.
- 1.2. Since the introduction of the DPA in 1998, technology, and how it is used to process data, has radically transformed the way organisations operate. To adapt to modern technology, in 2016, the EU adopted the General Data Protection Regulation (GDPR). It replaces the 1995 Data Protection Directive and came into effect on 25 May 2018.

- 1.3. The GDPR is employed across the EU and Member States and incorporated within the UK's government Data Protection Bill. The act:
 - 1.3.1. • Reflects modern, digital practices for handling data. The Bill also allows the Information Commissioners Office (ICO) power to bring criminal proceedings against offences of malpractice;
 - 1.3.2. • Contains local derogations allowed by GDPR as seen in UK Law;
 - 1.3.3. • Introduces two offences within the UK, the:
 - 1.3.3.1. • 'Re-identification of de-identified personal data' - the matching of de-identified data with publicly available information in order to identify the individual to which the data belongs to;
 - 1.3.3.2. • 'Alteration of personal data to prevent disclosure' - this offence criminalises the alteration of personal data after a subject access request has been filed with a data controller.
- 1.4. Data Protection Bill can be found at www.gov.uk/guidance/data-protection-bill-overview
- 1.5. In the UK, the GDPR will be overseen by the ICO. The ICO is an independent public body set up to uphold information rights in the public interest. The ICO sit independently of government, though are sponsored by the Department for Digital, Culture, Media and Sport (DCMS). The ICO will have powers to take action where organisations are failing to comply with the law; as indeed the ICO do currently with the existing Data Protection laws. The ICO also has powers under the Privacy and Electronic Communications Regulation (PECR) which governs the use of electronic means of marketing such as emails, text messages, etc., which was updated in 2016.
- 1.6. Personal Data is simply identified as 'Personal' if it is concerned with identifiable living individuals, irrespective of the data being processed automatically, electronically or manually; and recorded 'Data' (not unrecorded conversations with service users, donors or customers).
- 1.7. GDPR defines 'Personal Data' as - any information relating to an individual or identifiable natural person (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, an online identifier, or to one or more of the factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person). For data to be classified as sensitive personal data it must fall into the following categories:
 - 1.7.1. • The racial or ethnic origin of the subject
 - 1.7.2. • The subject's political opinions
 - 1.7.3. • The subject's religious beliefs or beliefs of a similar nature
 - 1.7.4. • Whether the subject is a member of a trade union
 - 1.7.5. • Information on the subject's physical or mental health condition
 - 1.7.6. • Information on the subject's sexual life
 - 1.7.7. • The commission or alleged commission of an offence by the data subject
 - 1.7.8. • Information relating to the commission or alleged commission of an offence by the data subject. The Special Categories now specifically includes Biometric Data and Genetic Data where processed to uniquely identify an individual. (e.g., fingerprint payment systems).

- 1.8. Valid reasons for processing the data are:
 - 1.8.1. • The individual whom the personal data is about has consented to the processing;
 - 1.8.2. • The processing is necessary: in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract;
 - 1.8.3. • The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract);
 - 1.8.4. • The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident;
 - 1.8.5. • The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions;
 - 1.8.6. • The processing is in accordance with the "legitimate interests" condition.

2. Conquest Data Protection Policy Overview

- 2.1. Compliance with the GDPR is a legal requirement and is to be followed at all times by Conquest Equestrian Centre (NB: Charity - 'Conquest Centre Ltd' and Business - 'Conquest Equestrian Centre Ltd'. Both hereafter known as **'Conquest'**), its staff, volunteers, contractors, trustees, sponsors or other parties working on behalf of Conquest (hereafter known as **'Data Processors'**). This Policy sets out the obligations of Conquest regarding the protection of personal data and the rights of staff, trustees, clients, volunteers, sponsors, donors, customers, suppliers, and partners (hereafter known as **'Data Subjects'**). This Policy does not form part of an employee's contract of employment and may be amended at any time. Conquest places high importance on the correct, lawful, and fair handling of all personal data respecting the legal rights, privacy and trust of all individuals with whom it deals.
 - 2.1.1. • The scope of Conquest's Data Protection Policy covers the following information:
 - 2.1.1.1. • What data Conquest keeps and why it keeps this data
 - 2.1.1.2. • To what types of data the policy applies
 - 2.1.1.3. • Identify who at Conquest is responsible for processing the data
 - 2.1.1.4. • The main data risks faced by Conquest
 - 2.1.1.5. • Key precautions to keep data protected
 - 2.1.1.6. • How data should be stored and backed up
 - 2.1.1.7. • How Conquest ensures data is kept accurate and when data will be deleted
 - 2.1.1.8. • What to do if an individual asks to see their data and when Conquest will turn down a Subject Access Request
 - 2.1.1.9. • Under what circumstances Conquest discloses data, and to whom
 - 2.1.1.10. • How Conquest keeps individuals informed about data it holds
 - 2.1.1.11. • The role of Conquest's Data Protection Officer
 - 2.1.1.12. • Who is responsible for reporting any breaches to the ICO and Charity Commission

3. Conquest's Commitment

- 3.1. Conquest agree that all confidential and personal identifiable information concerning the staff, clients, volunteers, customers, suppliers and partners

(hereafter known as '**Personal Data**') will be held securely and in confidence using appropriate technical and organisational measures. Conquest is committed to compliance with General Data Protection Regulation (EU) 2016/679 (hereafter called '**GDPR**') and relevant UK and EU data protection legislation in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Conquest collects and processes. Specifically, Personal Data:

- 3.1.1. • Must be processed lawfully, fairly and in a transparent manner in relation to individuals' rights
- 3.1.2. • Shall be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes of statistical purposes will not be considered to be compatible with the initial purposes
- 3.1.3. • Must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- 3.1.4. • Has to be accurate and kept up to date. Every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which that are processed is erased or rectified without delay
- 3.1.5. • Must be kept in a form which permits identification of all persons associated with Conquest for no longer than is necessary for the purposes for which the personal data is processed. Personal data will be deleted after a set period if the Data Subject has had no data activity over a set period of time - with the exception of

Data Subject	Deleted Data if Inactive for (yrs)
Staff	7
Trustee	3
Client	1
Volunteer	1
Sponsor	10
Donor	10
Customer	1
Supplier	7
Partner	3

- 3.1.6. Storage of personal data may be stored for longer periods in the interests of accident/incident recording subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the Data Subject;
- 3.1.7. Is to be processed ensuring appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Processing Personal Data

- 4.1. Conquest collects and processes Personal Data (Reference - <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>) directly from Data Subjects and/or from third parties

and will only process the Data for the specific purposes set out in this Policy. GDPR identifies that the Data Subject has the right to:

- 4.1.1. • Be informed
- 4.1.2. • Have access to their data
- 4.1.3. • Reflect on the data provided
- 4.1.4. • Have data erased (also known as the 'right to be forgotten')
- 4.1.5. • Restrict their data being processed
- 4.1.6. • Data portability
- 4.1.7. • Object and have their data used for automated decision-making or profiling

- 4.2. The purposes for which Conquest processes Personal Data will be communicated to the Data Subject at the time of their Personal Data collection, where it is collected directly from them, or as soon as possible after Data is collected from a third party. Conquest will:
 - 4.2.1. • Process Personal Data during the term of the Agreement, unless otherwise agreed by the Data Subjects and will be a Data Processor in accordance with the GDPR
 - 4.2.2. • Only act on the written instructions of the Data Subjects (unless required by law to act without such instructions)
 - 4.2.3. • Process personal data on behalf of the Data Subjects to fulfil the contract obligations to provide pre-employment screening services on their behalf
 - 4.2.4. • Only screen the Data Subjects to the screening level agreed to and ordered by the individual concerned
 - 4.2.5. • Process personal identifiable information under instruction from the Data Subjects. The information collected about the data subject will be limited to what is necessary to fulfil the Data Subjects involvement with Conquest. The information may include:
 - 4.2.5.1. • Name/previous names
 - 4.2.5.2. • Current address/previous addresses
 - 4.2.5.3. • Date of birth - age - gender
 - 4.2.5.4. • Medical information
 - 4.2.5.5. • Criminal record
 - 4.2.5.6. • Qualifications, institutes of study, personal and professional references
 - 4.2.5.7. • Current and past employments
 - 4.2.5.8. • Identification documents
 - 4.2.6. • Ensure any access by partners or third parties working with Conquest will be subject to the same conditions and must provide the same level of protection for the fundamental rights of the data subject;
 - 4.2.7. • Hold Personal Data securely in the UK;
 - 4.2.8. • Not sell Personal Data to third parties, nor copy or disclose Data to any third-party other than those required to conduct the service entered into by the organisation;
 - 4.2.9. • Recognise Data Subjects at Conquest as Data Controllers in their own right. Therefore, when processing Personal Data, a Data Controller is obligated to comply with the GDPR.
 - 4.2.10. • Seek to make the following information available to the Data Subject:
 - 4.2.10.1. • Details of Conquest and name of the Data Protection Officer;
 - 4.2.10.2. • The purpose of the Personal Data being collected - if required, the legal basis and legitimate interests justifying the data collection;
 - 4.2.10.3. • Where Personal Data is not obtained directly from the Data Subject, the scope of the Personal Data collected and processed;

- 4.2.10.4. • Where Personal Data has been transferred to one or more third party, details of those parties;
- 4.2.10.5. • Details of the length of time the Personal Data will be held by Conquest;
- 4.2.10.6. • Details of the Data Subjects rights under GDPR;
- 4.2.10.7. • Details of the Data Subject's rights to withdraw their consent to Conquest's processing of their Personal Data at any time;
- 4.2.10.8. • Details of the Data Subject's right to complain to the ICO;
- 4.2.10.9. • Details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it;
- 4.2.10.10. • Details if any automated decision-making that will take place using the Personal Data, including information on how decisions will be made, the significance of those decisions and any consequences.
- 4.2.11. • Not transfer Personal Data outside of the European Economic Area (EEA) without the explicit consent from the Data Subject and only after they have been informed of the possible risks of such transfer. Data transferral will only be done outside the UK if there is an appropriate "level of protection for the fundamental rights of the data subjects" For this to happen specified safeguards apply including EU acceptance of adequacy, membership to Privacy Shield, acceptance of model contract clauses, binding corporate rules or the assessment of adequacy by Conquest.

5. Personal Data Management

- 5.1. Personal information about the Data Subjects will be held by Conquest for the duration of their association with Conquest. After this period the information will be deleted so that it is beyond use with the exception of specific data that refers to incidents and accidents. That data will contain the minimum amount of information required as reference information required for future legal and medical claims. Conquest takes appropriate organisational and technical measures to ensure the security, data protection and privacy of data processed by Conquest on behalf of the Data Subjects. This includes alignment to ISO27001, ISO22301, BS10012, ISO9001, ISO14001 and Cyber Essentials. All reasonable steps are taken to protect Personal Data against unauthorised, unlawful processing and against accidental loss, destruction or damage. Personal Data consent will be given by each data subject; they will be provided with details of how to access Conquest's Data Protection Policy and/or, in the case of Volunteers, Students, Clients, Donors and Sponsors, asked to agree with the Conquest's Data Protection Policy statement (Appendix A - Data Consent).
- 5.2. Conquest will ensure that Data Processors will comply with GDPRs. GDPR seeks to ensure that personal data is processed lawfully, fairly and transparently without adversely affecting the rights of the data subject. GDPR requires the processing of data if at least one of the following applies:
 - 5.2.1. • The Data Subjects have given consent to the processing of his or her personal data for one or more specific purposes;
 - 5.2.2. • Processing is necessary for the performance of a contract to which Data Subjects is a party or in order to take steps at the request of the data subject prior to entering a contract;
 - 5.2.3. • Processing is necessary for the compliance with a legal obligation to which Conquest is subject;

- 5.2.4. • Processing is necessary to protect the vital interests of the data subject or of another natural person;
- 5.2.5. • Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Conquest;
- 5.2.6. • Processing is necessary for the purpose of the legitimate interests pursued by Conquest or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

- 5.3. All Personal Data will be kept accurate and up to date. The accuracy of the Personal Data will be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date Personal Data is found, all reasonable steps will be taken to amend or erase that Personal Data as appropriate. Personal Data inaccuracies will be amended within one month and the Data Subject informed of its completion.

- 5.4. **Data Portability.** Where Data Subjects have given their consent to Conquest for the processing of their Personal Data in such a manner or the processing is otherwise required for the performance of a contract between Conquest and the Data Subject, Data Subjects have the legal right under GDPR to receive a copy of their Personal Data and to use it for other purposes.

- 5.6. To facilitate the right of data portability, Conquest will make available all applicably Personal Data to Data Subjects and, where technically feasible and if requested by the Data Subject, Personal Data will be sent directly to another Data Controller.

- 5.7. Data Subjects have the right to object to Conquest processing their Personal Data based on legitimate interests, advertising, direct marketing including profiling and statistical purposes. Where a Data Subject objects to Conquest processing their Personal Data:
 - 5.7.1. • On legitimate interests, Conquest will cease such processing forthwith, unless it can be demonstrated that Conquest's legitimate grounds for such processing over-rides the Data Subject's interests, rights and freedoms, or the processing is necessary for the conduct of legal claims;
 - 5.7.2. • For direct marketing purposes, Conquest will cease such processing forthwith;
 - 5.7.3. • For statistical purposes, the Data Subject must, under GDPR, demonstrate grounds relating to their particular situation. Conquest is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

- 5.8. Profiling is used by Conquest to evaluate certain personal aspects of an individual i.e., to analyse the performance at work, health, personal preferences, reliability, movement etc and provide information to Donors and funders/supporters. Where Conquest uses Personal Data for profiling purposes, the following will apply:
 - 5.8.1. • Clear information will be provided to the Data Subject explaining the profiling, including its significance and likely consequences;
 - 5.8.2. • Appropriate and mathematical or statistical procedures will be used;
 - 5.8.3. • Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected will be implemented;

- 5.8.4. • All Personal Data will be secured in order to prevent discrimination effects arising out of profiling.
- 5.9. If requested by the Data Subjects, Conquest shall permanently destroy all confidential information held in its possession or under its control except for specific data that refers to incidents and accidents. That data will contain the minimum amount of information required as reference information required for future legal and/or medical claims.

6. Data Subject Access

- 6.1. Conquest shall assist a Data Subject in providing subject access requests (SAR) using Conquest's 'Subject Access Request Form' (at Appendix B) and allowing data subjects to exercise their rights under the GDPR. SARs will:
- 6.1.1. • Be forwarded to the Data Protection Officer or the Conquest Manager within 24 hours of receipt;
- 6.1.2. • Be assessed for viability and should it be deemed manifestly unfounded, excessive or adversely affect the rights and freedoms of others, Conquest will refuse the request;
- 6.1.3. • Not draw down a financial fee; however, Conquest reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.
- 6.2. Conquest shall assist Data Subjects with audits and inspections, providing them with information they need to ensure that Conquest and the individuals are meeting their obligations under GDPR Article 28. In addition, Conquest will inform Data Subjects if Conquest are asked to do something infringing the GDPR or other UK, EU or member state data protection law.
- 6.3. Conquest will assist the Data Subject, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.
- 6.4. Conquest will co-operate with supervisory authorities (such as the Information Commissioner's Office (ICO)) in accordance with GDPR Article 31 and will keep records of its processing activities in accordance with GDPR Article 30.2.
- 6.5. Conquest will notify any personal data breaches to Data Subjects in accordance with GDPR Article 33
- 6.6. Conquest employs a data protection officer as required by GDPR Article 37.
- 6.7. Data Subjects are to acknowledge that Conquest is reliant on them for direction as to the extent to which Conquest is entitled to use and process their Personal Data. Consequently, Conquest will not be liable for any claim arising from any act or omission by Conquest, to the extent that such act or omission resulted directly from the Data Subjects instructions.

7. Data Protection Officer

- 7.1. The UK mandates a requirement to appoint a Data Protection Officer (DPO) in certain situations. Conquest's DPO is created because Conquest:
 - 7.1.1. • Is a Charitable organisation;
 - 7.1.2. • Processes data activities which involve regular monitoring of data subjects covering a large range of data topics;
 - 7.1.3. • Employs a core activity processing sensitive personal data.
- 7.2. The Conquest DPO will keep written internal records of all Personal Data collection, holding and processing methods. They are accountable for the following information:
 - 7.2.1. • The recording of Conquest's DPO and any third-party data controllers;
 - 7.2.2. • The purposes for which Conquest processed Personal Data;
 - 7.2.3. • Details of the scope of Personal Data collected, held and processed by Conquest and how the Personal Data relates to the Data Subject;
 - 7.2.4. • Details of any third parties that will receive Personal Data from Conquest and on what basis. A copy of any agreement requesting the transfer Personal Data must be kept and reviewed prior to signing to ensure processing provisions are compliant with GDPR. The DPO is to be integrally involved in all Conquest contract negotiations;
 - 7.2.5. • Details of how long Personal Data will be retained by Conquest;
 - 7.2.6. • Detailed descriptions of all technical and organisational measures taken by Conquest to ensure the safety of Personal Data.
- 7.3. Conquest will undertake a Privacy Impact Statement (at Appendix C) on Personal Data and overseen by the DPO. The DPO will address the following:
 - 7.3.1. • The purpose(s) for which Personal Data is being processed and the processing operations to be carried out on that Personal Data;
 - 7.3.2. • Details of the legitimate interests being pursued by Conquest;
 - 7.3.3. • An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
 - 7.3.4. • An assessment of the risks posed to individual Data Subjects;
 - 7.3.5. • Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of Personal Data, sufficient to demonstrate compliance with GDPR.

8. Data Protection Measures

- 8.1. Conquest Information Systems - Acceptable Use Policy. Data Processors will maintain IT security by protecting the confidentiality, integrity and availability of Personal Data as defined in Conquest's IT Policy. All Conquest Data Processors shall comply with the following when working with Personal Data:
 - 8.1.1. • All Conquest Data Processors must use their issued Conquest 365 email address for all work involving Personal Data. The use of personal email addresses for this purpose is strictly forbidden;
 - 8.1.2. • Where any Personal Data is to be erased or disposed of it should be done securely. Hardcopies are to be shredded and electronic copies are to be deleted securely using the procedures detailed in the IT Policy
 - 8.1.3. • Transmission of Personal Data should use secure networks only;

- 8.1.4. • Personal Data contained in an email should be stored securely and the email, and any temporary files associated with the email, is to be deleted;
- 8.1.5. • Where Personal Data is sent by facsimile transmission, recipients are to be informed in advance and be awaiting the receipt of the Personal Data at the point of delivery;
- 8.1.6. • Hardcopy Personal Data should be passed directly to the recipient;
- 8.1.7. • Disclosure of Personal Data may be shared with any member of Conquest providing there is a legitimate need to do so;
- 8.1.8. • No Personal Data may be shared to other parties without the authorisation of the Conquest Manager and/or the DPO;
- 8.1.9. • All hardcopies of Personal Data, along with electronic copies stored on removable media, should be stored securely in a suitable lockable container;
- 8.1.10. • Personal Data must be handled with care at all times and should not be left unattended or on view by unauthorised persons;
- 8.1.11. • Personal Data users must ensure that individual monitors do not show confidential information to others and that they log off from their PC, or other device, when it is left unattended;
- 8.1.12. • If using a laptop, tablet computer, memory stick, smartphone, other mobile device or an approved personal device, Data Processors must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on any equipment to protect confidential data in the event of loss or theft. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport. NB: Personal data regarding individuals should only be removed from the office on portable devices where it has been encrypted so that it is protected if that device is lost or stolen;
- 8.1.13. • All Personal Data process and stored electronically will use accredited software, password protected and will be backed up - as detailed in the Conquest IT policy;
- 8.1.14. • All passwords protecting Personal Data should be changed regularly - passwords are to contain a combination of uppercase and lowercase letters, numbers and symbols. Passwords are not to be recorded and, if forgotten or changed, reset by approved methods as detailed in the Conquest IT Policy;
- 8.1.15. • Updates to Conquest PCs and devices are applied as required by the IT Manager. Privately owned devices used for Conquest work must be regularly updated by the owner;
- 8.1.16. • Downloads or the installation of software on to Conquest systems from external sources are not permitted without the authorisation of the IT Manager.
- 8.1.17. • Data collection techniques including 'cookies' should be revised to ensure that excessive data collection is not occurring and that automated deletion processes are in place to remove Personal Data after a set period of time.

9. Conquest Data processes

- 9.1. Conquest is to ensure the following measures are taken with respect to the collection, holding and processing of Personal Data:
 - 9.1.1. • Data Processors are to be made aware of their individual responsibilities Conquest's Data Protection and are to comply with the Policy at all times;
 - 9.1.2. • Personal Data will only be accessed by Conquest Data Processors in order to carry out their duties;
 - 9.1.3. • Data Processors will receive training and advice as to how to handle Personal Data;
 - 9.1.4. • Personal Data used by external bodies will be appropriately supervised, authorised and are to follow GDPR principles;
 - 9.1.5. • Data processing will be regularly monitored, audited and reviewed.
 - 9.1.6. • Data Processors will be evaluated and reviewed regularly.

10. Data Breaches

- 10.1. A personal data breach is defined as “a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.” If Conquest has a personal data breach, the Data Breach Checklist and Assessment Form (Appendix D) is to be enacted which will:
 - 10.1.1. • Investigate the data breach and perform an initial assessment as to the severity of the incident;
 - 10.1.2. • Notify internally and, if necessary, identify who to notify externally. Conquest is to ensure that a robust breach detection, investigation and internal reporting procedures are in place. Following ICO's guidance, both the Regulator/Supervisory Authority and Data Subject will be notified within 72 hours of the data breach using Conquest's 'Data Breach Reporting Form' (Appendix E) and recorded on the Data Breach Register (Appendix F). Further reference to the latest ICO reporting policy can be found at: www.ico.org.uk/for-organisations/report-a-breach/.
- 10.2. Along with reporting a data breach to the ICO, Conquest will also need to consider whether the data breach is a serious incident, and if so whether to report to the Charity Commission - further direction can be found at <https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity>. Data breaches are classed serious when:
 - 10.2.1. • Conquest's data has been accessed by an unknown person; this data was accessed and deleted, including the charity's email account, donor names and addresses;
 - 10.2.2. • A Conquest laptop, containing personal details of beneficiaries or staff, has been stolen or gone missing and it's been reported to the police;
 - 10.2.3. • Conquest funds lost due to an online or telephone 'phishing scam', where trustees were conned into giving out bank account details;
 - 10.2.4. • A Data Protection Act breach has occurred and been reported to the ICO.
- 10.3. Data breach notifications will include:
 - 10.3.1. • Categories and number of Data Subjects concerned;
 - 10.3.2. • Types and number of Personal Data records concerned;
 - 10.3.3. • Contact details of Conquest DPO;
 - 10.3.4. • Likely consequences of the data breach;

- 10.3.5. • Identification of the measures taken to address the breach and what has been done to mitigate its possible diverse effects.

11. Fundraising

- 11.1. Conquest primarily operates an income generation scheme using donors, sponsorship and fundraising (hereafter known as 'Funders'). The minimum amount of Personal Data of Funders is retained by Conquest, it is stored securely and processed only by those Data Processors authorised as part of their job description to do so. Conquest will not pass on Funders Personal Data to third parties.
- 11.2. Collection of Funders Personal Data will clearly identify the:
- 11.2.1. • Funders consent - consent must be unambiguous, freely given, demonstrable, specific and informed;
- 11.2.2. • Justification for the need of financial contributions;
- 11.2.3. • Opt-in, opt-out options;
- 11.2.4. • Funders rights are protected, and information is available as to:
- 11.2.4.1. • Why Personal Data is collected;
- 11.2.4.2. • What is done with the Personal Data;
- 11.2.4.3. • How Personal Data is shared - if at all;
- 11.2.4.4. • How Personal Data is stored;
- 11.2.4.5. • When Data Subjects can access their Personal Data.
- 11.2.5. • Personal Data retention duration;
- 11.2.6. • Personal Data disposal instructions.
- 11.3. Personal Data will be retained by Conquest for six years to satisfy Gift Aid and HMRC requirements, but other Personal Data may be retained indefinitely depending on the Funders background and potential for continuing financial support of Conquest. Funders Personal Data will be monitored regularly. Information on Fundraising can be found at: <http://bit.ly/IOFGDPR>.

12. Managing Financial Data

- 12.1. Financial data of Data Subjects are held securely by Conquest and is accessed only by authorised Conquest Data Processors. Financial Personal Data records are kept manually and electronically and cover:
- 12.1.1. • Conquest staff records, including salary, tax and pension records;
- 12.1.2. • Volunteer Personal Data (as required);
- 12.1.3. • Client Personal Data including financial records;
- 12.1.4. • Supporter and Funders data including donations, support provided and any additional financial linked data i.e., copies of cheques, bank details, property, livery and equipment purchases;
- 12.1.5. • Suppliers' information, including email addresses or contact information of those that are providing goods or services to Conquest - including bank details;
- 12.1.6. • Beneficiary financial data, such as grants made or financial assessments.
- 12.2. Personal Financial Data will be retained by Conquest for a period of 7 years (tax purposes). Data Subjects have rights to complain (4.2.10.8), maintain their individual rights (2.1.1) and are able to initiate a SAR (6.1); additionally,

detailed information about bank details will be reviewed annually and any financial data no longer relevant will be deleted. Data Subjects Financial Data is to be used for legitimate purposes only.

- 12.3. Conquest's financial controller will use Personal Data to generate reports, track their production, disseminate the reports according to their usage and use assured disposal processes when the financial reports are no longer required.

13. Beneficiary Data

- 13.1. Client/beneficiary Personal Data held by Conquest, both manual and electronic, needs to be clearly identified and understood. Consent must be agreed and recorded before any Personal Data is obtained. The beneficiary must understand:
- 13.1.1. • What Personal Data is held, including the duration of time that they are to be held. Beneficiaries consent must be specific, informed, withdrawn and at any time, freely given, involve clear affirmative action and be verifiable;
 - 13.1.2. • The location and types of Personal Data held and what work has been undertaken to obtain and cleanse the records;
 - 13.1.3. • That Personal Data held may constitute sensitive data, especially in relation to Personal Data relating to children and medical conditions;
 - 13.1.4. • The process by which the Personal Data has been obtained, including, whether there is a duplicate between electronic and locally held records;
 - 13.1.5. • The implications of providing financial data such as grants, financial assessments and/or salary records;
 - 13.1.6. • The individuals responsible for the Personal Data at each stage of the process.
- 13.2. Personal Data of beneficiaries may be obtained through a variety of methods in order to increase Conquest's performance and effectiveness. Whichever method is used in the acquisition of Personal Data consent is to be achieved, they retain their right to complain (4.2.10.8), the maintain their individual rights (2.1.1) and their ability to initiate a SAR (6.1).
- 13.3. Under GDPR Article 8(2), Conquest will need to make 'reasonable efforts' to verify that consent has been given or authorised for the collation of children's Personal Data from their parent, guardian, carer or 'the holder of parental responsibility' except when Conquest needs to process children's Personal Data in relation to preventative or council services that directly affect the child.

14. Policy Review

- 14.1 The Data Protection Officer is responsible for monitoring and reviewing this policy. This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or government advice may trigger interim reviews.

Appendix:

- A Data Consent.
- B Subject Access Request Form.
- C Privacy Impact Statement.**
- D Data Breach Checklist and Assessment Form.

E Data Breach Reporting Form.
F Data Breach Register

Appendix A

Data Consent Information

INTRODUCTORY STATEMENTS: (located on registration, application and donation forms)

Client Registration Form: We will use the information you provide on this form to make sure Conquest Centre provides the best possible service to you and to fulfil our legal obligations.

Volunteer Application Form: We will use the information you provide on this form to fulfil our legal obligations with regard to your work as a volunteer at Conquest Centre and also to fulfil our obligations to the vulnerable people we work with.

Donation/Gift Aid Form: We will use the information you provide on this form to process your donation and fulfil our legal obligations for example with regard to Gift Aid.

PERSONAL CONTACT DETAILS: (where-ever we are gathering data such as names, addresses, contact telephone numbers etc)

Donation/Gift Aid Form: The contact information you provide will only be used to communicate with you with regard to your donation. We will only contact you with other information if you consent to being added to our e-mail mailing list (in the box provided).

All other forms: The contact information you provide will be used as needed to communicate with you with regard to the services you receive from Conquest Centre. We will only contact you with other information if you consent to being added to our e-mail list in the box provided.

E-MAILING LIST: (where-ever we are gathering consent to add people to our e-mail mailing list)

We use our e-mailing list to send you very infrequent information on Conquest Centre's work, events and fundraising activities. We will never pass your details to anyone else. Should you wish to be removed from our e-mailing list at any time either unsubscribe using the link or let us know at info@conquestcentre.org.uk or call 01823 433614.

SHARING NON-PERSONAL DATA: (where-ever we are gathering information about you including date of birth, medical conditions or disabilities etc)

Donation/Gift Aid Form: In accordance with our Data Protection Policy, we may share **non-personal**, statistical or summary information (e.g., information which could never be linked to an individual) with funders and other organisations interested in our work e.g., through summary information on annual donations in our Annual Report.

Riding For The Disabled (RDA) tracker forms: The information you give us on this form will be used to provide **non-personal**, statistical or summary information for funders and other people interested in our work – for example to say how many Conquest Centre clients have improved their confidence through our work. This means that any information or feedback quotes you provide will only be used in a way that it is **anonymous**.

All other forms: **NON-PERSONAL DATA:** As a Charity we need to provide information on 'users' of our services in order to gain funding. The information shared is always **non-personal**, which means it could never be linked back to an individual. In accordance with our Data Protection Policy we may, for example, share generalised information on the number of users registered, age groups and/or types of medical conditions.

Suggested replacement for above “NON PERSONAL DATA” paragraph: In accordance with our Data Protection Policy, we may share **non-personal**, statistical or summary information (e.g., information which could never be linked to an individual) with funders and other organisations in order to gain funding- for example the number of users registered, age groups and/or types of medical conditions.

HOW YOUR DATA IS STORED: (where-ever we are gathering information about you)

Riding For The Disabled (RDA) tracker forms: The data collected on the form will be uploaded to the RDA Tracker, but only Conquest Centre will be able to see the personal data such as name and date of birth.

Your information may be stored on other ‘third party servers’, for example we use Microsoft 365, but wherever it is stored we are committed to protecting your privacy as legally required and take appropriate security measures to safeguard your data and prevent any unauthorised access to it.

All other forms: Your information may be stored on a ‘third party server’, for example we use Microsoft 365, but wherever it is stored we are committed to protecting your privacy as legally required and take appropriate security measures to safeguard your data and prevent any unauthorised access to it. We will only pass your information on to third parties when we are legally required to do so – for example if required by the local authority.

For more detail on how your information is used, how we maintain the security, and your rights to access information we hold on you, please contact info@conquestcentre.org.uk

PHOTO’S/QUOTES/CASE STUDIES/PUBLICITY ON INDIVIDUAL DONATIONS ETC:
(where-ever we are gathering consent to use identifiable information)

We will use your.....photograph/words...to help demonstrate Conquest Centre’s work to funders and other interested parties. This may include use on social media and in the press. We will not use surnames or any other information about you which is not included here. If you want us to stop using your...photograph/words...at any time just let us know by contacting info@conquestcentre.org.uk

If you have any concerns, or would like more detail on how your information is used, how we maintain the security, and your rights to access information we hold on you, please contact info@conquestcentre.org.uk

Appendix B

Subject Access Request Form

Should you wish to access certain information held about you, please complete this form and return it to the Conquest Centre Data Protection Officer by email or hard copy. This is permitted under the General Data Protection Regulations (GDPR).

If you require help in assessing the Data held about you call Jessica Dixon (Centre Manager) or speak to the Conquest Centre Data Protection Officer on 01823 433614.

Person making the request:		Address:	
Contact telephone number:		Scope of Data requirement:	

By completing this form you are making a request under the GDPR for information held about you by Conquest Centre that you are eligible to receive.

Required information:

Please include all detail relating to the information you seek. This includes any relevant dates, names of individuals who may hold the information, types of information (electronic and/or hard copy) to assist us in locating your information.

By signing this document, you indicate that you are the Data Subject named above. Conquest Centre cannot accept requests from anyone else regarding your personal data. We may need to contact you for further identifying information before proceeding with your request.

Please note: should your request for Personal Data be deemed manifestly unfounded, excessive or adversely affect the rights and freedoms of others, Conquest Centre will refuse the request.

Data Subject' signature of person making the request:		Date:	
--	--	--------------	--

Please keep one copy and return on copy via email to the Conquest Centre Data Protection Officer.

Appendix C

Appendix D

Data Breach Checklist/Assessment Form

1. Initial Assessment of incident:

Guidance: as soon as possible you should take steps to contain the breach and recover lost data, but before you can do this, we will need to make a preliminary assessment of what data has been lost, why and how.

Summary of the facts:	<i>Provide as much information as possible</i>
Scope and approximate number of Personal Subjects Concerned:	
Scope and approximate type of Personal Data Concerned:	
Any other comments:	

2. Incident Management Team:

Team Member Name	Conquest Job Title
	DPO

3. Background information:

Name of person notifying the actual or suspected breach:	
Name of Supervisor:	

Date of actual or suspected breach:	
Date of discovery of actual or suspected breach:	
Date actual or suspected breach notified to Conquest DPO:	

4. Assessment of Breach and Potential Harm:

Guidance: Conquest Data Protection Policy defines Personal Data and categories of a Data Breach. The Conquest DPO is to complete and assessment of the actual or suspected Data breach

Assessment of facts:	
Number of Personal Data records concerned:	
Classify the sensitivity of the Data breach:	
Identify the cause of actual or suspected breach or incident:	
Assess the potential harm or distress for Data Subjects:	
Assess the potential harm to Conquest Centre:	
Explain what actions have been undertaken:	
Explain what actions are to be undertaken to mitigate the actual or suspected data breach or incident:	

Please keep one copy and return one copy via email to the Conquest Centre Data Protection Officer.

Appendix E

Data Breach Reporting Form

This form is to be used to report details of an actual or suspected data breach at Conquest Centre.

Please answer the questions below as fully as you can and then email the form to the Data Protection Officer at your earliest convenience and no later than 24 hours of the actual or suspected breach being identified. Please refer to the Conquest Centre Data Protection Policy for further guidance.

If you believe the Data Breach to be urgent call Jessica Dixon (Centre Manager) or speak to the Conquest Centre Data Protection Officer on 01823433614.

Person making the report:	
Role/position at Conquest Centre:	
Contact telephone number:	
Date of the Report:	

Date of actual or suspected data breach:											
Date of discovery of actual or suspected data breach:											
Summary/description of data breach: <i>Provide as much information as possible, including the amount, sensitivity and type of data involved.</i>											
Identify the confidentiality breach i.e., employee, client, volunteer, sponsor, student or a combination of all data? <i>Describe the nature of the breach i.e., what format was the material that has been identified as a data breach and what was the scope of the data:</i>	<table> <tr> <td>Employee</td> <td>Yes/No</td> </tr> <tr> <td>Client</td> <td>Yes/No</td> </tr> <tr> <td>Volunteer</td> <td>Yes/No</td> </tr> <tr> <td>Sponsor</td> <td>Yes/No</td> </tr> <tr> <td>Student</td> <td>Yes/No</td> </tr> </table>	Employee	Yes/No	Client	Yes/No	Volunteer	Yes/No	Sponsor	Yes/No	Student	Yes/No
Employee	Yes/No										
Client	Yes/No										
Volunteer	Yes/No										
Sponsor	Yes/No										
Student	Yes/No										
Cause of suspected breach: <i>Provide a detailed account of what happened.</i>											
Is the actual or suspected data breach ongoing? <i>If yes, explain why/what.</i>	Yes/No										
Who is or could be affected by the actual or suspected breach? <i>Include detail of the type of data breach and approximate number of data subjects concerned. NB. Do not notify affected data subjects - Conquest DPO will determine the notification protocols.</i>											
Are you aware of any related or other data breaches? <i>If yes, list your concerns.</i>	Yes/No										

--	--

Please keep one copy and return on copy via email to the Conquest Centre Data Protection Officer

