

The Open College of Equine Studies

General Data Protection Regulation (GDPR) Policy

Introduction

From 25.05.18 General Data Protection Regulation (GDPR) regulates the way in which all personal data is held and processed. Due to the nature of the business TOCES needs to collect and use information about people with whom we work. This includes current, past and prospective employees, freelance tutors, lecturers and prospective and existing students.

TOCES is registered as a data controller on the register kept by the Information Commissioner's Office (ICO).

This policy sets out The Open College of Equine Studies' (TOCES') legal basis for holding personal data within specified categories. It explains what data we collect, how we store it and what we do with it. It explains the individuals' rights in terms of GDPR.

Its purpose is to ensure that everyone handling personal information at TOCES is fully aware of the requirements of GDPR and complies with data protection procedures and that data subjects (mainly students) are aware of their rights.

TOCES will ensure that:

- everyone managing and handling personal information understands that they are responsible for following good data protection practice
- this policy is available to all members of staff
- everyone managing and handling personal information is appropriately trained and supervised
- queries about handling personal information are promptly and courteously dealt with and clear information is available to all staff

Staff responsibilities for data protection and confidential information

- All staff should be aware of the requirements of the Act and how the rules apply to them.
- All staff must complete data protection induction and annual training.
- All staff have a responsibility to ensure that they respect confidential information in their possession and maintain information security.
- Disclosure of confidential information gained as a result of employment within TOCES to a third party is not permitted.
- All staff are responsible for ensuring personal information is kept no longer than is necessary.

This document will be reviewed and updated periodically.

LAWFUL BASIS

Data must be held under one or more of the lawful bases specified within GDPR.

TOCES holds peoples' personal data under three different lawful bases:

1. Lawful Basis of Contract
2. Lawful Basis of Legitimate Interest
3. Lawful Basis of Consent

1. Lawful Basis of Contract

The personal data of students, lecturers, tutors, veterinary practices, clinical coaches and employees is covered by the lawful basis of contract. The decision that the lawful basis upon which TOCES shall process these data is that of Contract was made on 29th April 2018.

Justification

The legal basis for holding this data is that of processing necessary for TOCES to comply with its contractual obligations.

GDPR Article 6(1)(b) states this is a lawful basis for processing where:

“processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”

I.e.:

1. You have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.
2. You haven't yet got a contract with the individual, but they have asked you to do something as a first step (e.g. complete an enrolment form) and you need to process their personal data to produce their Learner Agreement, Memorandum of Understanding, Lecturer/Tutor or Employment Contract (the Contract).

As the processing is necessary for our contract with the individual, processing is lawful on this basis and separate consent is not needed.

Where is this basis relied upon?

- Learner Agreement between the learner and TOCES
- Memorandum of Understanding between veterinary practices and TOCES
- Lecturer/Tutor Contract
- Employment Contract

How are individuals informed of this?

- GDPR Compliance Notification Email
- GDPR Notice on websites
- Privacy Notice on websites and Moodle Learner Platform

- Enrolment Form
- Addendum to Learner Agreement
- Addendum to Memorandum of Understanding
- Addendum to Lecturer/Tutor Contract
- Addendum to Employment Contract

What information do we collect?

Students: Name, address, email address, telephone numbers, date of birth, academic and professional qualifications, payment method details, e.g. credit/debit card details. At study weeks we request information about student health, e.g. allergies, that may affect the student while they are at TOCES.

Veterinary practices: Names of senior partners, practice managers and clinical coach. Practice address/es, email addresses, telephone numbers.

Employees, tutors and lecturers:

Name, address, email address, telephone numbers, curriculum vitae.

2. Lawful Basis of Legitimate Interest – business to business marketing

The personal data of veterinary practices, and clinical coaches working within these practices, is used to provide information about TOCES' veterinary nursing programmes and is covered by the lawful basis of Legitimate Interest. The decision that Legitimate Interest is the lawful basis upon which TOCES shall process this data was made on 29th April 2018.

Justification

On condition that consent is not required under Privacy and Electronic Communications Regulations (PECR), data can be used for marketing activities under "Legitimate Interests" provided the use of the data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object to what we are doing.

In line with Para 142 of the Information Commissioner's Office Direct Marketing publication the rules on consent, soft opt-in and the right to opt out do not apply to electronic marketing messages sent to 'corporate subscribers' which means companies and other corporate bodies e.g. limited liability partnerships.

However, in the interests of good practice, TOCES offers all its email marketing recipients the option to stop receiving information from TOCES.

Where is this basis relied upon?

- Email communications to veterinary practices promoting equine veterinary nursing training programmes.

How are individuals informed of this?

- GDPR Compliance Notification within the marketing email.

What information do we collect?

Veterinary practices: Practice and clinical coaches' email addresses.

3. Lawful Basis of Consent

The data of individuals who have expressed an interest in TOCES' courses via the website or email is covered under the lawful basis of Consent.

Justification

This data is used to notify and inform individuals of the courses on offer from TOCES. Consent is the most appropriate lawful basis for processing this data.

Consent is requested via the following email message:

“As you have previously expressed interest in our Equine Educational Courses we have your name and email address on our contact database. We'd like to keep you updated with details of the courses we offer and, as you are probably aware, we now need your express consent to be able to do this.

Please note that we will never share your data with third-parties for marketing, or other, purposes.

If you consent to us contacting you to let you know about TOCES' courses, please tick to confirm:

A. I wish to receive course information and updates from TOCES

You have the right to withdraw this consent at any time. This can be done by sending an email which includes your name and relevant email addresses, and has the subject CONSENT WITHDRAWAL, to admin@equinestudies.co.uk or by ticking the following box:

B. I do not wish to receive course information or updates from TOCES

If you tick box B above or we don't hear from you, we will remove your contact details from our database and will no longer send you information about our courses.”

DATA ADMINISTRATION

1. TOCES name and contact details:

The Open College of Equine Studies
33 Lower Green
Higham
Bury St Edmunds
IP28 6NJ
Tel: +44 (0) 1284 811 401

Email: info@equinestudies.co.uk

2. Contact details of our GDPR representative:

Julie Brega: Julie.brega@equinestudies.co.uk 01284 811 401

3. Data protection officer (DPO) status. TOCES has not appointed a DPO because under the GDPR, the following do not apply:

- The organisation is a public authority;
- Core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- Core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

4. The purposes of the processing. Data is processed to enable TOCES to:

- Respond to enquiries regarding our courses
- Enrol students onto courses
- Process payments
- Provide tutor and administrative support for the duration of the course
- Register learners with awarding bodies
- Provide information to students about study weeks
- Award and send out certificates upon course completion
- To notify potential students of upcoming enrolment deadlines
- Process RCVS training practice approvals
- Monitor clinical coach activities

5. Categories of personal data obtained where personal data is not obtained from the individual it relates to.

- Email addresses.

6. Recipients or categories of recipients of the personal data.

- TOCES administrative team
- TOCES tutor/s responsible for an individual student

7. Controller and processor contracts. There is a written contract between the GDPR Controller (TOCES) and those involved in the processing of data, the Processors (TOCES administration team).

8. **International data transfer.** TOCES will not transfer personal data to any third countries or international organisations.

9. **Retention periods.**

- Data is retained for seven years from the relevant student enrolment date.

10. **Individuals' rights.** The rights available to individuals in respect of the processing:

- Individuals can request sight of records held.
- Individuals can request deletion/amendment of data provided it does not impact TOCES' ability to carry out contractual obligations.
- Individuals can request confirmation that their data is being processed.

This information will be provided as quickly as possible, within one month of receipt of a request. The identity of the person making the request will be verified using 'reasonable means'. If the request is made electronically, the information will be provided in a commonly used electronic format.

11. **The right to lodge a complaint** with a supervisory authority.

- The individual can complain to Julie Brega by emailing Julie.brega@equinestudies.co.uk
- If you are still dissatisfied you have the right to contact the Information Commissioner's Office, the independent body overseeing GDPR compliance: <http://ico.org.uk/>.

12. **The source of the personal data** if the personal data is not obtained from the individual it relates to.

- Email addresses from business websites.

13. **Privacy Information Review**

We regularly review and, where necessary, update our privacy information. If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

14. **Rectification**

- The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- We have one calendar month to respond to a request.
- In certain circumstances we can refuse a request for rectification.

15. **Right to erasure**

Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement).

16. **Right to restrict processing**

Individuals have the right to request we restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and we are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim.

17. **Right to data portability.** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

18. **Right to object.** Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

19. **Security.** Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. We ensure that TOCES has a level of security that is 'appropriate' to the risks presented by our processing.

This has been calculated based on

- the nature and extent of TOCES' premises and computer systems;

- the number of staff and the extent of their access to personal data; and
- any personal data held or used by a data processor acting on TOCES' behalf.
- When considering physical security, we assess factors such as:
 - the quality of doors and locks, and the protection of premises by such means as alarms, security lighting or CCTV;
 - how we control access to premises, and how visitors are supervised;
 - how we dispose of any paper and electronic waste; and
 - how we keep IT equipment, particularly mobile devices, secure.

When considering cybersecurity, we appraise:

- system security – the security of network and information systems, including those which process personal data;
- data security – the security of the data we hold within systems, e.g. ensuring appropriate access controls are in place and that data is held securely;
- online security – e.g. the security of website and any other online service or application that we use; and

We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.

- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We have an information security policy and take steps to make sure the policy is implemented.
- Where necessary, we have additional policies and ensure that controls are in place to enforce them.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal data we process.
- We make sure that we can restore access to personal data in the event of any incidents, with a secure backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

Effective date: 24.05.18

Review 1 due date: 24.11.18