Data Protection Policy

University College of Osteopathy

Core Documentation Cover Page					
Data Protection Policy					
Version number	**Dates produced and approved (include committee)**	**Reason for production/ revision**	**Author**	**Location(s)**	**Proposed next review date and approval required**
V1.0	Mar 2018 SMT	Produced to: • Align with the new EU General Data Protection Regulation. • Supersede the separate Data Protection Policies for Students and Staff.	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	Mar 2020 Or in response to legislative changes
V2.0	Sep 2018 SMT	Major Amendments to reflect Data Protection Act 2018.	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	Sep 2020 Or in response to legislative changes

Equality Impact	
Positive equality impact (i.e. the policy/procedure/guideline significantly reduces inequalities)	
Neutral equality impact (i.e. no significant effect)	X
Negative equality impact (i.e. increasing inequalities)	

If you have any feedback or suggestions for enhancing this policy, please email your comments to: quality@uco.ac.uk

Data Protection Policy

CONTENTS

PART 1: DATA PROTECTION POLICY

1. INTRODUCTION

1.1 The University College of Osteopathy (UCO) is registered with the Information Commissioner's Office as a Data Controller (Registration Number: Z7454534). As such the UCO is responsible for the collection and maintenance of the personal data of its stakeholders, including students, staff and patients, in line with current data protection legislation.

1.2 Such legislation includes:

a) The Data Protection Act 2018 (DPA 2018)

b) The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)

1.3 The UCO takes the protection of all personal data extremely seriously and is fully committed to protect of the rights and freedoms of all individuals in relation to the processing of their personal data in compliance with this legislation.

1.4 The aim of this policy is to inform stakeholders of the UCO involved in processing personal data with their responsibilities under the DPA 2018 and GDPR and to set out the standards expected by the UCO in relation to processing personal data and safeguarding the personal data and rights of individuals.

2. SCOPE

2.1 The UCO's Data Protection Policy applies to all students and staff of the UCO. Any breach of the policy may result in the UCO, as the registered Data Controller, being liable in law for the consequences of the breach. Legal liability may also extend to the individual processing the data and their Head of Department or line manager under certain circumstances. In addition, breach of the UCO's Data Protection Policy by staff or students will be considered a disciplinary offence and will be dealt with according to the UCO's relevant disciplinary procedures.

2.2 Any member of staff or student who considers that the policy has not been followed with respect to personal data about themselves should raise the matter with the Data Protection & Freedom of Information Officer (DPFIO).

2.3 This policy applies to all personal data, including sensitive personal data, for which the UCO is responsible in whatever format it is (e.g. paper or electronic data, including databases, emails, photographs, video, CCTV and sound recordings).

2.4 Outside agencies and individuals who work with the UCO, and who have access to personal information for which the UCO is responsible, will be expected to comply with this policy and with the above data protection legislation.

3. LEGAL FRAMEWORK

A) THE DATA PROTECTION ACT 2018 (DPA 2018)

3.1 The DPA 2018 implements the UK government's manifesto commitment to update the UK's data protection laws to make them fit for purpose for the digital age. It also sets new standards for protecting general data in accordance with the GDPR whilst exercising a number of agreed modifications (derogations) to the GDPR to make it work for the benefit of the UK. In summary the DPA 2018:

- Makes our data protection laws fit for the digital age in which an ever-increasing amount of data is being processed.
- Empowers people to take control of their data.

- Supports UK businesses and organisations through the change.
- Ensures that the UK is prepared for the future after the UK has left the EU.

B) The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)

3.2 The GDPR is a regulation of the European Parliament, the Council of the European Union and the European Commission. Its main intent is to strengthen and unify data protection for all individuals within the European Union (EU).

3.3 The GDPR has direct effect across all EU member states meaning that the UCO must comply with the GDPR for most legal obligations subject to the provisions detailed in the DPA 2018. The GDPR and DPA 2018 must therefore be read side by side.

C) Complying with Data Protection Law

3.4 The GDPR sets out seven key principals which the UCO shall comply with:

a) Lawfulness, fairness and transparency; personal data shall be processed lawfully, fairly and transparently in relation to individuals.

b) Purpose limitation; personal data shall be collected for specified, explicit and legitimate purposes in a manner that is incompatible with those purposes.

c) Data minimisation; personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accuracy; personal data shall be accurate and kept up to date and that every reasonable step must be taken to rectify or erase inaccurate data without delay having regard to the purposes for which they are processed.

e) Storage limitation; personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

f) Integrity and confidentiality (security); personal data shall be 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.

g) Accountability; the data controller shall be responsible for, and be able to, demonstrate compliance with the GDPR.

3.5 In addition, the UCO shall respect the rights of individuals regarding their personal data in accordance with the GDPR which include:

a) The right to be informed (about the collection and use of their personal data including our purposes for processing their personal data, retention periods for that personal data and who it will be shared with).

b) The right of access to their person data (i.e. through a Subject Access Request).

c) The right to rectification (to have personal data rectified or completed if it is incomplete).

d) The right to erasure (or the right “to be forgotten” subject to exemptions specified in the GDPR).

e) The right to restrict processing (to store the personal data but not use it).

f) The right to data portability (to allow individuals to obtain and reuse their personal data for their own purposes across different services in a safe and secure way, without affecting its usability).

g) The right to object (to the processing of their personal data in certain circumstances).

h) Rights in relation to automated decision making and profiling (with no human involvement).

4. Personal Data

A) Personal Data

4.1 Under the DPA 2018 and GDPR personal data means data which relate to a living individual who can be identified:

a) from those data, or

b) from those data and other information (i.e. an identifier) which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual .

4.2 Personal data may include the following information:

- Name.
- Identification number.
- Address.
- Phone number.
- Email address.
- Other personal identifiers such as locations data or online identifier.

B) Sensitive Personal Data

4.3 Sensitive personal data (also referred to as “special category data” under the GDPR) is data that is more sensitive and therefore needs greater protection.

4.4 Sensitive personal data may include information about an individual’s:

- Race or ethnic origin.
- Political opinion.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
- Physical or mental health or condition.
- Sexual life or sexual orientation.
- Commission or alleged commission of any offence.
- Proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
- Genetics data.
- Biometric data (where used for identification purposes).

5. Privacy by Design

5.1 To comply with the DPA 2018 and the GDPR the UCO shall use a "privacy by design" approach when it develops any new projects or reviews current projects to consider any impacts on individuals' privacy appropriately and consistently by undertaking a Data Protection Impact Assessment (DPIA) as described in our Data Protection Impact Assessment Policy[1].

6. Registration with the Information Commissioner's Officer (ICO)

6.1 The UCO is registered with the Information Commissioner's Office (ICO) as a Data Controller (Registration Number: Z7454534) in line with the Data Protection (Charges and Information) Regulations 2018.

7. Responsibilities

A) The Information Governance & Security Steering Group (IGSSG)

7.1 The UCO's IGSSG on behalf of the Senior Management Team has oversight of planning and policy development in relating to information compliance, including data protection.

B) The Data Protection & Freedom of Information Officer (DPFIO)

7.2 The UCO has appointed a Data Protection & Freedom of Information Officer (DPFIO) to deal with data protection matters, including subject access requests, and who reports directly to the Board of Directors regarding these.

7.3 The main responsibilities of the DPFIO are to:

- Inform and advise the organisation and its employees about their obligations to comply with the DPA 2018, GDPR and other data protection laws.
- Monitor compliance with the DPA 2018, GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

7.4 The DPFIO also:

- Has professional experience and knowledge of data protection law.
- Reports to the Board of Directors.
- Operates independently and shall not be dismissed or penalised for performing their tasks.

7.5 The DPFIO is the first point of contact for:

- Queries regarding compliance with the UCO Data Protection Policy and current data protection and freedom of information legislation.
- Advice to UCO staff regarding data protection compliance.
- Subject access requests.
- Liaising with the Information Commissioner's Office (ICO), including preparation and submission of the UCO's annual data controller registration.

C) Heads of Department & Line Managers

7.6 Heads of Department and line managers are responsible for ensuring that the processing of personal data in their department conforms to the requirements of the DPA 2018, GDPR and this policy. In particular they should ensure that new and existing staff who are likely to process

[1] https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy

personal data are aware of their responsibilities regarding this. This includes ensuring that staff are aware of the requirements of this policy are provided with adequate training and that they shall actively promote data legislation compliance to their staff.

7.7 Heads of Departments and Line Managers should also ensure that correct information and records management procedures are followed in their departments, including compliance with the UCO's Records & Information Management Policy and Records & Information Retention Schedule.

7.8 Heads of Departments and Line Managers developing new projects shall undertake a Data Protection Impact Assessment (DPIA) if necessary in consultation with the DPFIO.

D) STAFF

7.9 When processing personal data, UCO staff must ensure that they abide by the DPA 2018 and GDPR, this policy and any related policies. Staff who are uncertain as to whether their processing of personal data meets these requirements should refer any queries to the DPFIO in the first instance.

7.10 All new staff are required to complete Data Protection training and existing staff should also attend the training if they have not done so before or require a refresher.

7.11 Staff are required to allow the UCO to process their personal data as described in our Privacy Notice for Staff: https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy

7.12 In respect of complying with data protection legislation staff are required to agree to comply with:

- Data Protection Policy
- Freedom of Information Policy
- Subject Access Request Policy & Procedure
- Records & Information Management Policy
- Records & Information Retention Schedule
- Information Security Policy
- Data Security Breach Management Policy

7.13 Staff are responsible for ensuring that the personal data the UCO holds about them is accurate and up-to-date by informing the UCO of any changes or errors when they occur.

7.14 Staff who process personal data in connection with their UCO employment are permitted to do so under the UCO's ICO registration. Staff must inform the DPFIO if any registered processing ceases or if they wish to process new data or existing data for a new purpose.

7.15 All staff who use personal data are expected to:

- Familiarise themselves with and abide by the above DPA 2018 and GDPR principles.
- Familiarise themselves with and abide by this Data Protection Policy and the associated Code of Practice.
- Understand what is meant by "sensitive personal data" and know how to handle such data.
- Contact the DPFIO if in any doubt about how to handle personal data.
- Undertake appropriate Data Protection training provided by the UCO as specified by their line manager.

7.16 Where academic researchers wish to process any personal data, they must carefully consider the data protection implications of the use of personal data in research before undertaking the research.

7.17 Staff undertaking research involving the processing of personal data should comply with the UCO's Research Governance & Integrity Policy.

7.18 The UCO is not responsible for any processing of personal data by staff which is not related to their employment with the UCO, even if the processing is carried out using UCO equipment and facilities.

7.19 Staff developing new projects shall undertake a Data Protection Impact Assessment (DPIA) if necessary in consultation with the DPFIO.

E) STUDENTS

7.20 Students are required to allow the UCO to process their personal data as described in our Privacy Notice for Applicants and Students: https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy

7.21 Students also agree to allow the UCO to process their personal data as outlined in the Student Contract.

7.22 In respect of complying with data protection legislation students are required to agree to comply with:

- Data Protection Policy
- Freedom of Information Policy
- Subject Access Request Policy & Procedure
- Records & Information Management Policy
- Records & Information Retention Schedule
- Information Security Policy
- Data Security Breach Management Policy

7.23 Students are also responsible for ensuring that the personal data the UCO holds about them is accurate and up-to-date and must inform the UCO of any changes or errors as soon as they occur by emailing registry@uco.ac.uk.

7.24 Where a student wishes to process personal data as part of their research project the student's supervisor must ensure that the UCO's data protection obligations can be met before the student's choice of project is approved. Research students undertaking research involving the processing of personal data should comply with the UCO's Research Governance & Integrity Policy.

8. USE OF PERSONAL DATA BY AGENTS, CONSULTANTS OR CONTRACTORS

8.1 Where a third party such as an agent, consultant or contractor is employed to process personal data on behalf of the UCO (e.g. a mailing agency undertaking a mailshot or an independent research marketing company undertaking market research) which involves the processing of personal data, the UCO remains the data controller of that data.

8.2 UCO staff involved in the employment of an agent, consultant or contractor must ensure that a written contract (i.e. a data processing agreement) is in place for the purchase of any such service which should specify terms and conditions including requirements for data protection compliance by agents, consultants or contractors processing personal data on behalf of the UCO.

8.3 Further guidance on appropriate terms for such a contract can be obtained from the DPFIO (dpfio@uco.ac.uk).