University College of Osteopathy

Data Protection Policy

For Staff

University College of Osteopathy

Core Documentation Cover Page					
Data Protection Policy for Staff					
Version number	**Dates produced and approved (include committee)**	**Reason for production/ revision**	**Author**	**Location(s)**	**Proposed next review date and approval required**
V1.0	Jan 2013 SMT	To protect the rights and privacy of individuals (includes students, staff and other individuals associated with the UCO) in accordance with the Data Protection Act and associated codes of practice issued by the Information Commissioner.	ICT Manager	All master versions will be held in: J:\0 Quality Team - Core Documentation Intranet	Jan 2015
V2.0	Jul 2017 PRAG Chair	Administrative Amendments to update institution name change from British School of Osteopathy to University College of Osteopathy.	ICT Manager	All master versions will be held in: J:\0 Quality Team - Core Documentation Intranet	Jan 2015

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 FOR STAFF

CONTENTS

1. Scope 4
2. Introduction 4
3. Data Held at the UCO 4
4. Definitions from the Data Protection Act 1998 5
5. The Data Protection Principles 5

1. SCOPE

1.1 The University College of Osteopathy (UCO) is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and other individuals associated with the UCO) in accordance with the Data Protection Act and associated codes of practice issued by the Information Commissioner.

2. INTRODUCTION

2.1 The UCO takes the privacy and security of its staff members' and students' data seriously. The policy applies to all staff and students at the UCO. For instance, staff owe a duty of care to the UCO when processing data about students, other employers or other individuals.

2.2 Any breach of the Data Protection Act 1998 or the UCO Data Protection policy is considered to be an offence and in that event, the UCO disciplinary procedures will apply. Similarly, other individuals and organisations working in conjunction with the UCO are required to comply with this policy.

3. DATA HELD AT THE UCO

3.1 The UCO requires specific information about certain individuals for administrative purposes such as:-

a) To administer and maintain staff records for the purposes of fulfilling the contract of employment (e.g. running the payroll);

b) To administer and maintain student records for the purposes of student selection; providing educational services; career services; student association services; alumni services (including fundraising and directory publication);

c) To maintain such records as may be required by legislation (e.g. health & safety and employment legislation);

d) To respond to any query that individuals may raise with UCO about matters relating to their employment, their education or any other matter;

e) To disclose information about staff and former staff members or students and former students to future employers for reference purposes;

f) To keep staff and former staff members informed (by post, telephone or e-mail) about matters relating to their employment or pension;

g) To keep students and alumni informed (by post, telephone or e-mail) about relevant matters relating to the UCO;

h) To use information about staff and students for the purposes of management planning and forecasting, research and statistical analysis;

i) To disclose information about individuals in response to legislative/ court orders.

4. Definitions from the Data Protection Act 1998

4.1 "Personal Data" This relates to the information that can lead to the identification of an individual. This covers names, addresses, telephone numbers of individuals. It also applies to the expression of opinion about the individual, and the intentions of the data controller in respect of that individual.

4.2 "Sensitive Personal Data" Requires stricter methods of data processing. This means data concerning a Data Subject's racial or ethical origin, political opinions, religious beliefs, trade union membership, health, sex life or criminal convictions.

4.3 "Data Controller" Refers to the UCO, as an organisation that processes data about Data Subjects, includes the decision on data processing methods.

4.4 "Data Subject" Any living individual who is the subject of personal data held by the UCO.

4.5 "Processing of Personal Data" Any operation related to data management such as: obtaining, recording, altering, amending, margining, recording, disclosing and destroying of personal data.

4.6 "Data Processor" means an external person or organisation (not part of the UCO) who processes Personal Data for the UCO.

4.7 "Third Party" Any individual/ organisation other than the data subject, the data controller (UCO) or its agents.

4.8 "Relevant Filing System" Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

5. The Data Protection Principles

5.1 Personal data must be obtained and processed fairly and lawfully.

5.2 The Data Controller must receive consent from the Data Subject to process the information. Subjects should be informed about the purposes of processing the information, possible disclosures to third parties and the length of time that data will be held.

5.3 Personal Data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.

5.4 Data obtained for specified purposes must not be used for a purpose that differs from those.

5.5 Personal Data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.

5.6 Data collected should only be used for the specific purpose.

5.7 Personal data shall be accurate and, where necessary, kept up-to-date.

5.8 Periodic reviews of data stores should be carried out to ensure al information is accurate. It is the responsibility of individuals to ensure that data held by the UCO is up-to-date. Individuals need to ensure that data held by the UCO is up-to-date. Individuals should notify the UCO of changes in personal circumstance so records can be amended.

5.9 Personal data shall be kept only for as long as necessary.

5.10 Redundant or out of date information should be deleted. Further guidance is available on request. An individual shall be entitled, at reasonable intervals and without undue delay or expense, to be informed by the Data Controller whether it holds Personal Data of which that individual is the subject; and to have such data corrected or erased.

5.11 Appropriate security measures must be taken against authorised access, alteration, disclosure or destruction of Personal Data, and against accidental loss or destruction of Personal Data.

5.12 Care should be taken with regard to data storage, for example: access to filing cabinets, screens and other computer equipment and back-up procedures. Control over computer passwords is an important aspect of data security and passwords should not be disclosed to others within or outside the UCO.

5.13 Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.14 Recipients, outside the EEA, should be advised of the Data Protection Principles. Subjects should be made aware if data will be transferred outside the EEA and warned that data protection legislation may not be adhered to as strictly as in the EEA.