Data Protection Policy

Data Protection Policy

CONTENTS

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 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.

1.3 The aim of this policy is to inform stakeholders of the UCO involved in processing personal data with their responsibilities under relevant data protection legislation 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 can be considered a disciplinary offence and may 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) by emailing dpfio@uco.ac.uk.

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. 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.

B) The UK General Data Protection Regulation (UK GDPR)

3.2 The UK GDPR is the retained law version of the EU General Data Protection Regulation ((EU) 2016/679), which came into effect on the 1st January 2021 following Brexit.

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

3.3 The EU 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).

3.4 The EU GDPR has direct effect across all EU member states.

3.5 Although the EU GDPR does not apply in the UK, the UCO has an obligation to comply with this legislation when dealing with any services it provides to EU residents, for example partner institutions located within member states of the EU.

D) Complying with Data Protection Legislation

3.6 The UK 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 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 appropriate data protection legislation.

3.7 In addition, the UCO shall respect the rights of individuals regarding their personal data in accordance with data protection legislation 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 In the context of data protection legislation, 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 (this is not an exhaustive list):

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

B) Special Category Data

4.3 Special Category data) is data that is more sensitive and therefore needs greater protection.

4.4 Special Category includes the following information:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

4.5 The UCO processes Special Category data as described in our Privacy Notices and our Appropriate Policy Document.

C) Criminal Offence Data

4.6 Criminal Offence data covers a wide range of data which includes specific criminal convictions, allegations, investigations, and proceedings in addition to broader criminal activity. It also includes personal data relating to:

- Unproven allegations.
- Information relating to the absence of convictions.
- Personal data of victims and witnesses of crime.
- Personal data about penalties.
- Conditions or restrictions placed on an individual as part of the criminal justice process.
- Civil measures which may lead to a criminal penalty if not adhered to.

4.7 To process Criminal Offence data the processing must be lawful, fair and transparent and comply with all other principles and requirements of the UK GDPR which means that:

a) A lawful basis under UK GDPR Article 6 must be identified for this processing; and

b) One of the conditions under DPA 2018 Schedule 1 must be met.

4.8 The processing of Criminal Offence data is likely to result in high risk of harm to individuals if appropriate safeguards and mitigation are not put in place to protect and process this data appropriately. Whenever Criminal Offence data is processed, a Data Protection Impact Assessment (DPIA) must be undertaken in line with the UCO's DPIA Policy and approved by the UCO's Information Governance and Security Steering Group (IGSSG).

4.9 The UCO processes Criminal Offence data as described in our Privacy Notices and our Appropriate Policy Document.

5. Record of Processing Activities (ROPA)

5.1 The UCO keeps a comprehensive record of its data processing activities in an electronic format to easily identify and monitor the type and nature of personal data we process.

5.2 The UCO's ROPA is regularly reviewed in line with this policy, in response to legislative changes, when new personal data is processed or when the existing processing of personal data changes.

6. Privacy by Design – Data Protection Impact Assessments

6.1 The UCO shall use a "privacy by design" approach when it develops any new or reviews existing projects, systems or processing of personal data to consider any impacts on individuals' privacy.

6.2 Where any processing of personal data is "likely to result in high risk" a Data Protection Impact Assessment (DPIA) in line will be undertaken in line with the UCO's Data Protection Impact Assessment Policy[1].

6.3 The UCO will consider carrying out a DPIA if it plans to carry out any:

a) Evaluation or scoring.
b) Automated decision-making with significant effects.
c) Systematic monitoring.
d) Processing of sensitive data or data of a highly personal nature.
e) Processing on a large scale.
f) Processing of data concerning vulnerable data subjects.
g) Innovative technological or organisational solutions.
h) Processing that involves preventing data subjects from exercising a right or using a service or contract.

6.4 The UCO will always carry out a DPIA if it plans to:

a) Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
b) Process special-category data or criminal-offence data on a large scale.
c) Systematically monitor a publicly accessible place on a large scale.

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

d) Use innovative technology in combination with any of the criteria in the European guidelines.
e) Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
f) Carry out profiling on a large scale.
g) Process biometric or genetic data in combination with any of the criteria in the European guidelines.
h) Combine, compare or match data from multiple sources.
i) Process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines.
j) Process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines.
k) Process children's personal data for profiling or automated decision-making or for marketing purposes or offer online services directly to them.
l) Process personal data that could result in a risk of physical harm in the event of a security breach.

6.5 The UCO will also carry out a new DPIA if it changes the nature, scope, context, or purposes of data processing.

6.6 A DPIA will normally be carried out at the earliest stage of a project, system or plan involving the processing of personal data to ensure that processing is carried out appropriately and meets data protection legislation requirements. Where the UCO decides not to carry out a DPIA, the reasons for this will be documented.

6.7 DPIAs will normally be monitored regularly and reviewed at least every two years or in response to a change in processing or legislative changes.

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

7.1 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.

8. Disclosing Personal Data

A) Subject Access Requests (SARs)

8.1 In line with UK GDPR Article 15 individuals have the right of access to their personal data.

8.2 Individuals may request a copy of their personal data from the UCO at any time and can do so verbally or in writing, including via social media; this is known as a "Subject Access Request" (SAR) and should be managed as such in line with the UCO's Subject Access Request Policy & Procedure:

https://www.uco.ac.uk/about-uco/who-we-are/subject-access-request-policy

8.3 If a staff member or student receives an SAR, the DPFIO (dpfio@uco.ac.uk) should be informed immediately to ensure that the correct information is provided to the requester within the time required for responding to an SAR under the data protection legislation (30 calendar days) in an appropriate format.

8.4 It is important to note that responding to a SAR may involve the disclosure or redaction of third-party personal data which must be considered on a case-by-case basis and may involve the application of legal exemptions set out in data protection legislation.

8.5 A record of the number and nature of SARs is maintained by the DPFIO for monitoring purposes.

B) Disclosing Personal Data to Third Parties

8.6 To protect the privacy of individuals whose data the UCO processes the disclosure of personal data to a range of third parties must be carefully considered.

8.7 Requests from a third party to confirm whether an individual is a student, patient or staff member of the UCO should not be disclosed even if the request is from a concerned other, the Police or a government agency; some individuals choose to have little or no contact with third parties including family members, friends and representatives of their home state (e.g. Embassies and High Commissions) and this is not for the UCO to determine. In such cases, the third party should be informed that the UCO can neither confirm nor deny this, take the details of the third party and forward their request on to the individual concerned (if they are a member of the UCO) for them to respond to.

8.8 In all cases, all requests for personal information by individuals or third parties should be sent to dpfio@uco.ac.uk to review and advise on how they should be responded to:

I) Telephone Requests

8.9 Personal data should not be provided to a third party over the telephone, including family members or friends, the Police, local authorities or other organisations and bodies.

8.10 This includes neither confirming nor denying that an individual is a student, patient, employee, etc. of the UCO.

8.11 Where a third-party requests personal data by telephone they should be asked to make their request in writing to the appropriate Line Manager. The Line Manager is responsible for verifying whether the request is legitimate, whether consent from the individual concerned is required, and whether the data can be released in line with data protection legislation.

II) Written Requests

8.12 All written requests from third parties requesting personal data must be verified.

8.13 Written requests from third parties (including organisations / bodies) must be provided on official headed paper and signed by an individual with appropriate authority.

8.14 Ideally written requests will cite the relevant data protection legislation exemption or other legislation which authorises the UCO to release the information, however this is not a requirement, and the UCO may need to evaluate whether the information can be released.

III) Types of Third-Party Requests

8.15 Requests for personal data may be made by a range of third parties, which may need to be considered and responded to in different ways set out below.

Family Members & Friends: The UCO has no obligation to disclose information about a student, patient or staff member to their family members or friends without their consent. Staff and students should not disclose, nor should they feel pressurised to disclose such information without the written consent of the individual involved. Where consent for disclosure is received, a record of the consent should be kept on the individual's file.

Colleagues: Due consideration should be given before disclosing or sharing personal data about another colleague, student, patient or relevant other with another colleague. Personal data should only be shared where there is a legitimate reason for doing so, for example to

enable them to carry out their role. The level of detail shared should also be considered, ensuring that the minimum amount and type of data is shared or that information is redacted where appropriate. Shared data must also be shared in a secure way (for example via a restricted shared folder or password protected file) and deleted appropriately.

THE POLICE: There is no general requirement to disclose personal data to the Police. However, an exemption applies under the DPA 2018 (Section 29) for the purposes of the prevention and detection of crime and taxation where the UCO can release personal information to the Police without consent in some circumstances. However, before any such disclosure is made, the Police will be required to provide the request in writing which should be signed by the investigating officer and verified by a senior ranking officer.

LOCAL AUTHORITIES: All requests from local authorities for the personal data of students must be made in writing on headed paper. Information provided should be limited to facts, such as name and attendance. Requests for any Special Category data will require the consent of the student involved. A record of the consent should be kept on the student's file.

OTHER EDUCATIONAL INSTITUTIONS: Requests from other educational institutions for the personal data of students must be made in writing on formal headed paper. Where a request is received from an institution formerly attended by a student, the student must consent to the release of this information, or the institution must provide verifiable justification under data protection legislation. The minimum amount of information should be provided, for example, attendance and award, although additional information may be provided depending on the nature of the request.

SPONSORS: The UCO should not disclose personal data to sponsors or sponsoring bodies (with the exception of Student Finance England to whom the UCO reports and shares personal data in line with the UCO's Student Privacy Notice) without the consent of the individual concerned or without verifying the existence of a contractual agreement between the sponsor and the individual concerned which permits disclosure of the information.

PROFESSIONAL / ACCREDITING BODIES: Where a course is accredited by a professional body, students are normally informed at registration that their name and final award, including any failures, will be disclosed to that body, If a professional body requests the personal data of an individual on an ad hoc basis the consent of the individual will be needed to release the data.

REGULATORY BODIES: As a Higher Education Provider the UCO is obliged to disclose personal data, for reporting purposes, for example to the Higher Education Statistics Agency (HESA) and to meet Office for Students requirements.

EMPLOYERS / RECRUITMENT AGENCIES: Where the UCO is asked for a reference about an individual, typically for employment purposes, this should be made in writing by the third-party and should be verified that this has been authorised by the individual concerned. Only information held by the UCO should be disclosed, which will typically consist of factual information.

CONFIDENTIAL REFERENCES PRODUCED BY THE UCO: Where a third-party or an individual requests a copy of a confidential reference produced by the UCO disclosure can be refused under the DPA 2018 where the reference relates to education, training or employment; appointing office holders; or providing any service.

REFERENCES RECEIVED BY THE UCO IN CONFIDENCE: Where a third-party or an individual requests a copy of a reference received by the UCO ***in confidence*** from another individual or organisation, the request for the reference to be disclosed can be refused as an exemption under the DPA 2018 (Schedule 2, Part 4, Paragraph 24). If the reference has not been received

in confidence, the consent of all individuals relating to the reference should be sought before the information is released, including the referee and the individual(s) to whom it related, or where consent cannot be sought personal information unrelated to the data subject should be redacted.

OTHER THIRD PARTIES: Where requests for personal data from third parties not listed above are received advice should be sought from the DPFIO before any data is released.

9. SHARING PERSONAL DATA

9.1 In this context data sharing relates to the sharing of personal data between organisations that are data controllers.

9.2 Data sharing between the UCO and another data controller will be undertaken in line with the Data Sharing Code of Practice published by the Information Commissioner's Office (ICO):

https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/

9.3 Where data will be shared in this context, a DPIA will normally be undertaken which will be approved by the IGSSG.

9.4 All data sharing agreements must be authorised by the Vice-Chancellor.

10. UCO DATA PROTECTION RESPONSIBILITIES

A) THE INFORMATION GOVERNANCE & SECURITY STEERING GROUP (IGSSG)

10.1 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)

10.2 The UCO has appointed a Data Protection & Freedom of Information Officer (DPFIO) to advise on data protection matters, including DPIAs, and subject access requests.

10.3 The main responsibilities of the DPFIO are to:

- Inform and advise the organisation and its employees about their obligations to comply with data protection legislation.
- Monitor compliance with data protection legislation, including managing internal data protection activities, advise on DPIAs, staff training and conducting internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).
- Liaise with the Board of Directors and senior management about data protection matters.

10.4 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.
- Advising UCO staff regarding data protection compliance.
- Responding to Subject Access Requests and Freedom of Information Requests.
- Liaising with the Information Commissioner's Office (ICO) on behalf of the UCO.

C) HEADS OF DEPARTMENT, SENIOR MANAGERS & LINE MANAGERS

10.5 Heads of Department, Senior Managers and Line Managers are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data protection legislation and this policy. They should ensure that new and existing staff who are

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

10.6 Heads of Departments, Senior Managers 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.

10.7 Heads of Departments, Senior Managers and Line Managers developing new projects are also responsible for undertaking a Data Protection Impact Assessment (DPIA) if necessary, in consultation with the DPFIO.

D) STAFF

10.8 When processing personal data, UCO staff must ensure that they comply with data protection legislation, 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 their Line Manager or the DPFIO.

10.9 All new staff are required to complete Data Protection training.

10.10 Existing staff should complete Data Protection training when required and at the minimum every two years.

10.11 Staff should be aware of how the UCO processes their personal data as described in the UCO's Privacy Notice for Staff: https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy

10.12 In addition to complying with data protection legislation, staff are also required to comply with the UCO's:

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

10.13 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.

10.14 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.

10.15 All staff who use personal data are expected to:

- Familiarise themselves with and abide by the legislative data protection 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 or as specified by their Line Manager.

10.16 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.

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

10.18 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.

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

E) Students

10.20 Students should be aware of how the UCO processes their personal data as described in the UCO's Privacy Notice for Applicants and Students: https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy

10.21 Students also agree to allow the UCO to process their personal data as outlined in the UCO's Student Terms & Condition.

10.22 In addition to complying with data protection legislation students are also required to comply with the UCO's:

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

10.23 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.

10.24 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.

11. Use Of Personal Data By Agents, Consultants Or Contractors

11.1 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.

11.2 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.

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

CORE DOCUMENTATION RECORD 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
V3.0	Jun 2022 IGSSG Oct 2022 SMT	Major Amendments to reflect legislative changes following Brexit.	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	Oct 2025 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