
# Appropriate Policy Document

# UCO Appropriate Policy Document

## Contents

# 1. Preamble

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

An APD should demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the UK General Data Protection Regulation (UK GDPR) Article 5 principles. In particular, it should outline retention policies with respect to this data (see Schedule 1 Part 4).

The UCO processes SC or CO data for different purposes, which are all covered by this APD; a separate APD for each condition or processing activity is not required in line with guidance published by the Information Commissioner's Office (ICO) and therefore this one document covers them all.

Policies and procedures which are relevant to all the identified processing are referenced where appropriate.

The APD sets out how we process SC and CO data and how long we will retain it for explaining our compliance with the data protection principles in line with Schedule 1 of the DPA 2018 (Special Categories of Personal Data and Criminal Convictions Etc. Data) and Article 6 (Lawfulness of Processing) and Article 9 (Processing of Special Categories of Data) of the UK GDPR, including how long we will retain it for.

In line with Article 30 of the UK GDPR (Records of Processing Activities) our Record of Processing Activities (ROPA) sets out:

(a) The condition for processing the data which is relied upon in line with Schedule 1 of the DPA 2018.

(b) How the processing satisfies Article 6 of the UK GDPR (lawfulness of processing); and

(c) Whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

This APD therefore complements our ROPA under Article 30 of the UK GDPR and provides SC and CO data with further protection and accountability (see Schedule 1 Part 4 paragraph 41.)

This APD will be kept under review and will be retained until six months after the date we stop the relevant processing.

If the ICO asks to see our APD we will provide it free of charge in line with Schedule 1 Part 4 Paragraph 40 of the DPA 2018.

This APD should be read alongside the ICO's Guide to the UK GDPR and has been produced using the ICO's Appropriate Policy Document template (ICO APD template / 20191104 / V1.0).

# 2. Introduction

The University College of Osteopathy (UCO) is a UK Higher Education Provider registered with the Office for Students (OfS) which specialises in osteopathic education and, as such, is a public authority.

The UCO is also a healthcare provider offering patients with access to high-quality but affordable, osteopathic care and healthcare in other disciplines. The UCO Clinic is a teaching clinic providing students with essential clinical experience under the expert supervision and guidance of experienced, qualified healthcare practitioners.

To enable the UCO to carry out the above functions, we process both Special Category (SC) and Criminal Offence (CO) data in accordance with Article 9 of the UK General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act (2018) (DPA 2018).

To lawfully process SC and CO data, both a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9 of the UK GDPR are required.

In addition, as stated in the Preamble, an Appropriate Policy Document (APD) must (in many cases) be in place when SC and CO data are processed as stated in Schedule 1 Part 4 of the DPA 2018.

In line with Schedule 1 Part 4 of the DPA 2018, this APD sets out what SC and CO data we process including:

(a) Our lawful basis for processing the SC and CO data in line with Article 6 (Lawfulness of Processing) of the UK GDPR.

(b) The condition for processing the SC and CO data in line with Article 9 (Processing of Special Categories of Data) of the UK GDPR

(c) The condition for processing the SC and CO data in line with Schedule 1 (Special Categories of Personal Data and Criminal Convictions Etc. Data) of the DPA 2018.

(d) How we ensure compliance of processing SC and CO data in line with Article 5 of the UK GDPR (Principles Relating to Processing of Personal Data), including how long we will hold the SC and CO data.

Some of the information contained within this document may be held in other documents and we have linked to and referenced these as appropriate.

# 3. Description of Data Processed

We process the following types of SC and CO data:

- Racial / Ethnicity
- Religious / Philosophical Beliefs
- Sex Life / Sexual Orientation
- Health / Disability Data

- Criminal Offence Data

We do not process the following types of SC data:

- Biometric Data
- Genetic Data
- Political Opinion Data
- Trade Union Membership Data

# 4. Schedule 1 Condition for Processing

Listed below are the DPA 2018 Schedule 1 conditions for processing upon which we are relying.

The following abbreviations are used:

SC = Special Category Data

CO = Criminal Offence Data

**a) DPA Schedule 1 Part 1 Paragraph 1 (Employment and Social Protection)**

Where the UCO needs to process SC/CO data for the purposes of performing its obligations or rights as an employer, or for guaranteeing the social protection of individuals.

**b) DPA Schedule 1 Part 1 Paragraph 2 (Health or Social Care Purposes)**

Where the UCO needs to process SC/CO data for the purposes of performing its obligations as a health care provider, or for assessing the working capacity of employees and students.

**c) DPA Schedule 1 Part 1 Paragraph 3 (Public Health)**

Where the UCO needs to process SC data for the purposes of performing its obligations as a health care provider in the public interest as carried out by health care professionals.

**d) DPA Schedule 1 Part 1 Paragraph 4 (Research, etc.)**

Where the UCO needs to process SC data for scientific research purposes.

**e) DPA Schedule 1 Part 2 Paragraph 8 (Equality of Opportunity or Treatment)**

Where the UCO needs to process SC data as the processing is monitoring equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained.

**f) DPA Schedule 1 Part 2 Paragraph 9 (Racial and Ethnic Diversity at Senior Levels of Organisations)**

Where the UCO needs to process SC data for the purposes of identifying suitable individuals to hold senior positions at the UCO and to promote or maintain diversity in the racial and ethnic origins of individuals who hold senior positions.

**g) DPA Schedule 1 Part 2 Paragraph 10 (Preventing or Detecting Unlawful Acts)**

Where the UCO needs to process CO data for the purpose of preventing or detecting unlawful acts.

**h) DPA Schedule 1 Part 2 Paragraph 11 (Protecting the Public Against Dishonesty)**

Where the UCO needs to process CO data to protect members of the public against dishonesty, malpractice, or serious improper conduct; unfitness or incompetence; mismanagement in the administration of a body or organisation; or failures in services provided by a body or association.

**i) DPA Schedule 1 Part 2 Paragraph 12 (Regulatory Requirements Relating to Unlawful Acts and Dishonesty)**

Where the UCO needs to process CO data to comply with, or assist other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act or has been involved in dishonesty, malpractice or other seriously improper conduct.

**j) DPA Schedule 1 Part 2 Paragraph 16 (Support for Individuals with a Particular Disability or Medical Condition)**

Where the UCO needs to process SC data to provide support to individuals with a particular disability or medical condition.

**k) DPA Schedule 1 Part 2 Paragraph 17 (Counselling)**

Where the UCO needs to process SC/CO data to provide confidential counselling, advice, or support or of another similar service provided confidentially.

**l) DPA Schedule 1 Part 2 Paragraph 18 (Safeguarding of Children and of Individuals at Risk)**

Where the UCO needs to process SC/CO data to protect an individual aged under 18 or aged over 18 and at risk, from neglect or physical, mental or emotional harm or protect the physical, mental or emotional well-being of an individual, only where, in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining the data subject's consent would prejudice the provision of the protection, and is necessary for reasons of substantial public interest.

**m) DPA Schedule 1 Part 3 Paragraph 29 (Consent)**

Where the individual has given consent to the processing of SC/CO data.

**n) DPA Schedule 1 Part 3 Paragraph 30 (Vital Interests)**

Where the UCO needs to process SC and CO data to protect the vital interests of an individual or where an individual is physically or legally incapable of giving consent.

# 5. Procedures for Ensuring Compliance with the Principles

## Accountability Principle

The UCO demonstrates its compliance with the data protection principles set out in Article 5 of the UK GDPR through the following measures and documents:

a) The UCO keeps a record of its data processing activities by maintaining an electronic record of our data processing activities (Record of Processing Activities (ROPA)) which details what personal data we process, how we process it in line with the DPA 2018 and UK GDPR and our means of keeping data secure.

b) The UCO has in place the following data protection policies:

   a) Data Protection Policy

   b) Data Protection Impact Assessment Policy

   c) Data Security Breach Management Policy

   d) Information Security Policy

   e) Records & Information Management Policy

   f) Subject Access Request Policy & Procedure

   These policies are made available publicly on the UCO's website here:

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

c) The UCO takes a 'protection by design and default' approach by undertaking Data Protection Impact Assessments (DPIAs) for uses of personal data that are likely to result in high risk to individuals' interest, and always when this data includes Special Category or Criminal Offence data. The UCO's Data Protection Impact Assessment Policy published here describes this approach:

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

d) When the UCO routinely and/or regularly shares data with third parties, we enter into data sharing agreements with Data Controllers and Data Processors which meet the provisions of Article 26 and Article 28 of the UK GDPR respectively and Chapter 5 of the UK GDPR when these transfers are made to third countries or international organisations,

e) The UCO implements appropriate security measures which are proportionate to the risk associated with the processing.

f) The UCO has appointed a Data Protection Officer (the Data Protection & Freedom of Information Officer) whose roles and responsibilities align to Section 4 of the UK GDPR and Chapter 4 Paragraph 69 of the DPA 2018.

g) Our Privacy Notices explain to individuals how and why their data is processed by the UCO, what their rights are, and how they can contact our DPO and the UK's regulatory and supervisory authority (the Information Commissioner).

Our Privacy Notices are made available on the UCO website here:

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

h) The UCO has Cyber Essentials certification providing assurance that we have appropriate cyber security measures in place.

## Principle (a): lawfulness, fairness and transparency

As a public authority we need to process SC and CO data for the substantial public interest conditions outlined in Section 4 of this APD to meet the requirements of legislation such as the Higher Education and Research Act (2017), the Equality Act (2010), the Health and Safety Act (1974), the Counter Terrorism and Security Act (2015), and legislation relating to safeguarding, and processing employment data to meet our legal obligations as an employer.

We provide clear and transparent information to individuals about why we process their personal data, including our lawful bases for processing in our Privacy Notices. This includes information about why we process SC and CO data. Our Privacy Notices are published here:

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

## Principle (b): purpose limitation

We process SC and CO data where it is necessary to meet the following purposes:

a) Equal opportunities monitoring, including statutory returns to the Higher Education Statistics Agency (HESA).

b) Certain courses of study, work or study placements or casual work opportunities where a Disclosure and Barring Service (DBS) check is required.

c) Supporting special arrangements, such as building access plans, study inclusion plans, reasonable adjustments for study or work, and mitigating circumstances applications.

d) Providing individuals with appropriate support in a counselling session.

e) Providing individuals with healthcare.

f) To allow us to fully investigate a complaint or grievance.

g) Recording sickness absence.

h) Complying with health and safety obligations.

i) Where processing is necessary to respond to an emergency situation.

j) Responding to binding requests or search warrants from courts, the government, regulatory or enforcement bodies.

k) To fully process job applications.

l) To fully process course applications.

m) For the prevention and detection of unlawful acts (e.g. incidents captured on CCTV).

n) To verify the good character, competence and integrity of senior managers, trustees / directors and staff.

o) To take necessary steps to ensure that a natural or legal person offering philanthropic support or other support to the UCO has not committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct.

We will only process SC and CO data for the listed purposes, and in accordance with a condition in Article 9 (processing of special categories of personal data) and Article 10 (processing of personal data relating to criminal convictions and offences) of the UK GDPR and Schedule 1 Parts 1-3 of the DPA.

We process some SC and CO data for purposes not covered in this APD. These conditions are:

a) Where we ask for your explicit consent to process SC and CO data.

b) For the purposes of preventative or occupational medicine.

c) Where processing is necessary to protect your vital interests.

d) For research, statistics and archival purposes.

We may process data collected for any one of these purposes (whether by us or another Data Controller), for any of the other listed purposes, so long as the processing is necessary and proportionate to that purpose.

We will not process any personal data for purposes which would be incompatible with the purpose for which the data was originally collected.

## Principle (c): data minimisation

We design our data collection forms and other data collection tools to ensure that we only collect the SC or CO data necessary to achieve the purpose which are set out in our Privacy Notices publicly available here:

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

Where we operate systems which cannot control the volume of SC data collected (i.e. CCTV) we take measures to minimise the volume of data processed. We only monitor public spaces with the minimum number of cameras needed to cover the area, and we operate a short retention period of 1 month from the date the footage is recorded.

We are satisfied that we collect and retain SC and CO data for long enough to fulfil our purposes. We collect enough but no more than we need in accordance with the data minimisation principle, and we only hold SC and CO data for the period set out in our retention policies.

Our retention schedule sets out the correct disposal action once records containing special category data are no longer required and is published here:

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

| Principle (d): accuracy |
| --- |
| When we identify data which is inaccurate or out of date, having due regard for the purpose for which the data was processed, we will take necessary steps to rectify, replace or erase it as soon as possible and within one month. If there is a specific reason we cannot rectify or erase the data, for instance because the lawful basis does not permit it, we will record the decision.<br><br>We provide processes and interfaces for staff, students and patients and others whose data we process to keep their personal data up to date, as well as issuing regular reminders to update or provide equalities monitoring data. |
| **Principle (e): storage limitation** |
| SC and CO data processed by us for the purposes set out above, in our Privacy Notices and for the purposes of employment or substantial public interest, will be retained for the periods set out in our Records & Information Retention Schedule.<br><br>The retention policy for record categories is determined by our legal and regulatory obligations, and our business requirements.<br><br>Our Records & Information Retention Schedule is publicly available here:<br><br>https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy |
| **Principle (f): integrity and confidentiality (security)** |
| All electronic data including that related to SC and CO data is hosted on a secure network, and on the secure servers of third-party cloud storage providers with whom we have contractual agreements.<br><br>All hard copy data including that related to SC and CO data is securely stored in locked cabinets and secured rooms where access is restricted to relevant staff.<br><br>Electronic and hard copy data is managed according to our Records and Information Management Policy published here:<br><br>https://www.uco.ac.uk/about-uco/who-we-are/policies-procedures-and-privacy |

# 6. Retention and Erasure Policies

Our retention period for records containing SC and CO data that we process can be found in our Records & Information Retention Schedule.

Our disposal actions for records containing SC and CO data that we process can be found in our Records & Information Management Policy.

Both are publicly available here:

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

# 7. APD Review Date

This policy will be retained for the duration of the processing, and for a minimum of 6 months thereafter.

This policy will normally be reviewed annually or revised more frequently if necessary.

## Core Documentation Record Page

### Appropriate Policy Document

| Version number | Dates produced and approved (include committee) | Reason for production/ revision | Author | Location(s) | Proposed next review date and approval required |
|---|---|---|---|---|---|
| V1.0 | Nov 2022<br>SMT | Produced to align with UK Data Protection Legislation. | DPFIO | All master versions will be held with:<br>UCO Quality Team<br>Website | Nov 2023 |