College of Integrated Chinese Medicine Data Protection Policy

---

1.INTRODUCTION

1.1 The College of Integrated Chinese Medicine (CICM) is registered with the Information Commissioner's Office as a Data Controller (Registration Number: Z8468925). As such CICM 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 the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)

1.3 CICM 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 CICM involved in processing personal data with their responsibilities under the DPA 2018 and GDPR and to set out the standards expected by CICM in relation to processing personal data and safeguarding the personal data and rights of individuals.

2. SCOPE

2.1 CICM's Data Protection Policy applies to all students and staff of CICM. Any breach of the policy may result in CICM, 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 line managers under certain circumstances. In addition, breach of CICM's Data Protection Policy by staff or students will be considered a disciplinary offence and will be dealt with according to CICM'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 Management Committee.

2.3 This policy applies to all personal data, including sensitive personal data, for which CICM 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 CICM, and who have access to personal information for which CICM 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 numberof 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 CICM 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 CICM 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, CICM 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 CICM 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.

6. REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICER (ICO)

6.1 CICM is registered with the Information Commissioner's Office (ICO) as a Data Controller (Registration Number: Z8468925) in line with the Data Protection (Charges and Information) Regulations 2018.

7. RESPONSIBILITIES

7.1 CICM's Management Committee has oversight of planning and policy development in relating to information compliance, including data protection.

7.2 The Joint Principal is the first point of contact for:

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

7.3 Programme leaders and line managers are responsible for ensuring that the processing of personal data in their area of responsibility 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 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.

7.4 Programme leaders and line managers should also ensure that correct information and records management procedures are followed in their areas of responsibility, including compliance with CICM's Records keeping and communication.

7.5 When processing personal data, CICM 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 Joint Principal in the first instance.

7.6 Staff are required to allow CICM to process their personal data.

7.7 Staff are responsible for ensuring that the personal data CICM holds about them is accurate and up-to-date by informing CICM of any changes or errors when they occur. 7.8 Staff who process personal data in connection with their CICM employment are permitted to do so under CICM's ICO registration. Staff must inform the Joint Principal if any registered processing ceases or if they wish to process new data or existing data for a new purpose.

7.9 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
- Understand what is meant by "sensitive personal data" and know how to handle such data
- Contact the Joint Principal if in any doubt about how to handle personal data
- Undertake appropriate Data Protection training provided by CICM as specified by their line manager.

7.10 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.

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

E) STUDENTS

7.12 Students are required to allow CICM to process their personal data.

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

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

- Data Protection Policy
- Freedom of Information Policy

7.15 Students are also responsible for ensuring that the personal data CICM holds about them is accurate and up-to-date and must inform CICM of any changes or errors as soon as they occur by emailing admin@cicm.org.uk.

7.16 Where a student wishes to process personal data as part of their research project the student's supervisor must ensure that CICM's data protection obligations can be met before the student's choice of project is approved.

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 CICM (e.g. a mailing agency undertaking a mailshot or an independent research marketing company undertaking market research) which involves the processing of personal data, CICM remains the data controller of that data.

8.2 CICM staff involved in the employment of an agent, consultant or contractor must ensure that there is a written undertaking stating the requirements for data protection compliance by agents, consultants or contractors processing personal data on behalf of CICM.