International Kinesiology College

Website Date Collection and Privacy Policy

I have read the IKC data collection and privacy policy and agree to abide by its terms and conditions.

Objective

1.1 As part of its functions, IKC is required to receive and process relevant Personal Data regarding kinesiology students.

1.2 This policy sets out our commitment to protecting Personal Data, and particularly how we will ensure that:

(a) IKC staff understand how to handle data they have access to as part of their work; and

(b) IKC certified kinesiology instructors understand how to handle data they have access to as part of the provision of their services to kinesiology students.

Scope

1.3 This policy applies to anyone who obtains Personal Data that is controlled or processed by or on behalf of IKC. This includes and is not limited to IKC employees and IKC certified kinesiology instructors.

1.4 This policy applies regardless of where the Personal Data is held or whether it is held manually or electronically.

Definitions

1.5 "APA" means Privacy Act, 1988 (Aust).

1.6 "DPA" means Data Protection Act, 1998 (UK).

1.7 "Data Sharing Agreement", means an agreement that sets out the framework for the sharing of Personal Data.

1.8 "GDPR" means General Data Protection Regulation, 2016 (EU).

1.9 "Information Governance Team" means persons established by IKC to oversee data protection compliance.

1.10 "Personal Data" means any data or information, in paper or digital format, relating to a living individual. It includes but is not limited to names, contact details, financial details, course details and appropriate personal circumstances, and also Sensitive Personal Data. It does not include information that is already in the public domain.

1.11 "Personnel" means IKC employees, IKC certified kinesiology instructors and anyone else who obtains Personal Data that is controlled or processed by or on behalf of IKC.

1.12 "Privacy Impact Statement" means an analysis of the likely impacts of a project upon the privacy rights of individuals.

1.13 "Sensitive Personal Data" is defined in the DPA and includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings.

1.14 "Subject Access Request" means a request by an individual for access to Personal Data.

1.15 "processing" or "processed" in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making it available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

Data Protection Principles

1.16 IKC will comply with the DPA and GDPR principles as well as the Information Privacy Principles of the APA.

1.17 Any Personal Data received by IKC will be used solely for the IKC's internal database, record of classes taken, student progressions and other lawful purposes.

1.18 IKC will not disclose, sell or share any Personal Data with any third party or external agency on any occasion without the express consent of the individual to whom the Personal Data relates.

1.19 For the purposes of GDPR, IKC will ensure that Personal Data is:

(a) processed fairly and lawfully and in a transparent manner;

(b) obtained for one or more specified, explicit and lawful purposes;

(c) adequate, relevant and only limited to what is required;

(d) accurate and where necessary kept up to date;

(e) not kept in a form which permits identification of data subjects for longer than is necessary;

(f) processed in accordance with the rights of data subject;

(g) processed in a manner that ensures appropriate security of the Personal Data; and

(h) not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal information.

General requirements

1.20 IKC will comply with general requirements under the DPA and GDPR, including that:

(a) Personal Data should only be accessed by those who need to, for work or legitimate business purposes;

(b) Personal Data should not be divulged or discussed except when performing normal work duties or providing normal professional service;

(c) Personal Data must be kept safe and secure at all times, including at the office, public areas, home or in transit;

(d) Personal Data should be regularly reviewed and updated; and

(e) queries about data protection, internal and external, to the IKC must be dealt with effectively and promptly

1.21 IKC will take appropriate technical and organisational steps to ensure the security of Personal Data.

1.22 All Personnel (who are known to IKC) will be made aware of this policy and their duties under the DPA.

1.23 IKC and all Personnel are required to respect the Personal Data and privacy of others. They must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to Personal Data.

1.24 An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, Personal Data must be stored in appropriate systems.

Information Sharing

1.25 Personal Data may need to be shared with other organisations in order to deliver services or perform our duties. This can only be done where we have permission or there is legal obligation for us to share.

1.26 Personal Data can be shared within the IKC or with other third parties and the sharing can be:

(a) "Systematic" or routine information sharing where there is an established purpose; or

(b) "Exceptional" or one-off decisions, for example in conditions of real urgency.

1.27 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties. They are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

1.28 All Data Sharing Agreements must be signed off by a member of the Information Governance Team. IKC will keep a register of all Data Sharing Agreements.

2 Privacy Impact Assessments

2.1 Privacy Impact Statements will be completed in the following situations that involve Personal Data:

(a) at the beginning of a new business project or when implementing a new system that may affect the processing of Personal Data ;

(b) before entering into a Data Sharing Agreement; and

(c) when major changes are introduced into a privacy system or process.

3 Subject Access Requests

3.1 IKC recognises that access to Personal Data held about an individual is a fundamental right provided in the DPA.

3.2 IKC will ensure that all requests from individuals to access their Personal Data are dealt with as quickly as possible and within the timescales allowed in relevant legislation.

3.3 Individuals must submit Subject Access requests in writing (including by electronic methods) and provide any necessary proof of identification and required fee as part of the request.

4 Complaints

4.1 Anyone who feels that IKC has broken data protection law in any way, can complain. Examples of this are when they believe their information has not been obtained fairly, it has not been handled securely or they have asked for a copy of their information and they are not happy with IKC's response.

4.2 IKC will endeavour to ensure that all Personal Data held in relation to an individual is accurate. Individuals who consider that data is inaccurate or out of date may also request, in writing, that the information be corrected or erased. They will receive a written response indicating whether or not the IKC agrees and if so, the action to be taken. IKC will rely on individuals to provide accurate and

complete Personal Data when completing any enrolment or registration form or otherwise providing information to IKC or Personnel.

4.3 Individuals can also ask IKC to stop handling their Personal Data if they believe this will cause them harm or distress. IKC will act reasonably in relation to such request.

Training

4.4 Data Protection training is important so that all Personnel understand their responsibilities.

4.5 All IKC employees (including temporary employees) will receive mandatory internal training annually.

4.6 Other Personnel are encouraged to attend online training.

Non Compliance

4.7 Serious breaches of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action and may even lead to criminal prosecution.

4.8 Where those breaching this policy are not employees, this may be regarded as a serious breach of contractual obligations.

Policy Review

4.9 IKC has established an Information Governance Team.

4.10 Information Governance Team comprises the IKC President, IKC Registrar, and any officer or member of IKC to whom data protection functions are delegated from time to time.

4.11 Information Governance Team has direct responsibility for co-ordinating the maintenance and review of this policy annually.

4.12 Reviews will take into account changes in legislation, best practice, lessons learnt and may be in consultation with any relevant IT service providers or industry professionals.

Further Information and guidance

4.13 Enquiries regarding this policy should be directed to the Information Governance Team by using any of the contact details of the IKC set out in its website.