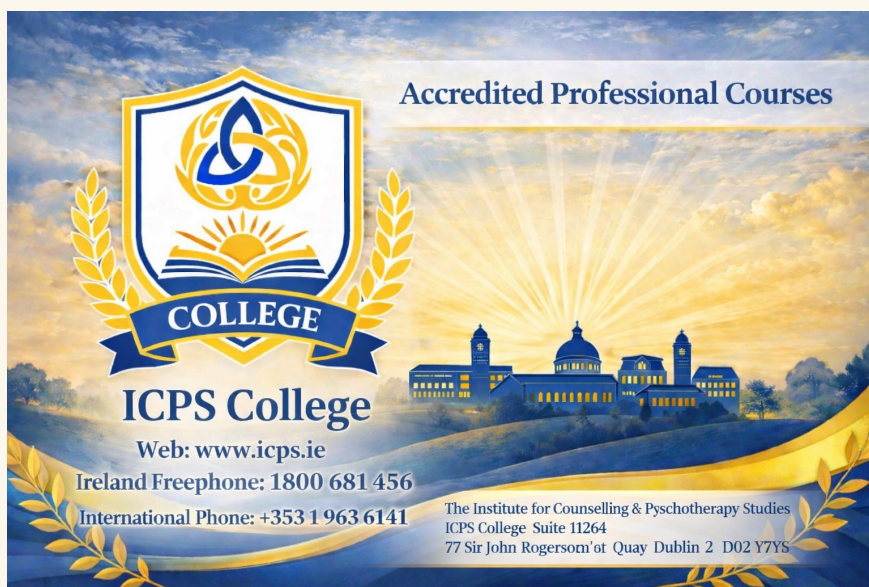


ESTABLISHED IN IRELAND • ACCREDITED PROFESSIONAL EDUCATION



Privacy Policy

for Educational Services

The Institute for Counselling & Psychotherapy Studies

ICPS College

Effective Date: 23rd May 2021

Last Updated: 1st February 2025



www.icps.ie • Freephone: 1800 681 456 • International: +353 1 963 6141



© ICPS College 2026–2030 • All Rights Reserved

1. Introduction

The Institute for Counselling & Psychotherapy Studies (hereinafter referred to as “ICPS,” “the Institute,” “the College,” “we,” “us,” or “our”) is fully committed to safeguarding the privacy, confidentiality, and security of all personal data entrusted to us by students, prospective students, applicants, course participants, alumni, website visitors, and other data subjects with whom we engage in the course of delivering our educational programmes. This commitment is rooted not only in our legal obligations under the General Data Protection Regulation (Regulation (EU) 2016/679) (hereinafter “GDPR”) and the Data Protection Act 2018 of Ireland, but also in the educational and ethical standards that govern the delivery of accredited diplomas, certificates, and continuing professional development programmes (Quality and Qualifications Ireland [QQI], 2022; Higher Education Authority [HEA], 2023).

As a provider of accredited educational and continuing professional development programmes, we recognise that the personal data we process in connection with enrolment, study, and assessment is important and must be handled with care. Such data may include details concerning a learner’s identity, academic history, prior qualifications, learning needs, course progress, assessment outcomes, and financial transactions (Department of Education, 2022). For this reason, we apply robust technical and organisational safeguards and consistent ethical standards to every stage of the data lifecycle, from initial enquiry and enrolment through to secure destruction once retention requirements have expired (Information Commissioner’s Office [ICO], 2023).

This Privacy Policy explains, in clear and accessible language, how we collect, use, store, share, and protect personal data when you visit our website at www.icps.ie; make enquiries about our courses, diplomas, certificates, or



continuing professional development offerings; submit an enrolment or booking form; access our online learning environment or virtual classroom; communicate with our administrative or academic staff by telephone, email, or written correspondence; or otherwise interact with our organisation in any educational capacity. By engaging with our educational services, you acknowledge that you have read, understood, and accepted the practices described in this Privacy Policy.

2. Data Controller and Contact Information

For the purposes of the GDPR and the Data Protection Act 2018, the Data Controller responsible for your personal data is the Institute for Counselling & Psychotherapy Studies. The registered correspondence address is Suite 11264, 77 Sir John Rogerson's Quay, Dublin 2, D02 Y7Y5, Republic of Ireland. Data protection enquiries, subject access requests, and other formal communications regarding the processing of personal data should be directed to GDPR@icps.ie. General educational enquiries may be made on our Free-Phone number 1800 681 456 or by email to education@icps.ie. We endeavour to acknowledge all data protection enquiries within five working days and to provide a substantive response within the statutory timeframe of one calendar month, as required under Article 12 of the GDPR (European Parliament and Council, 2016).

3. Legal Basis for Processing Personal Data

Under Article 6 of the GDPR, all processing of personal data must be supported by at least one identifiable lawful basis. The Institute relies on the following lawful bases, as determined by the nature of the data and the educational purpose of processing.

3.1 Personal Data (Article 6 GDPR)

We process ordinary personal data on one or more of the following legal bases. First, we may rely on consent under Article 6(1)(a), where you have given clear, specific, informed, and unambiguous indication of your wishes by means of a statement or affirmative action signifying agreement to processing, such as ticking a consent box on an enrolment form or subscribing to our newsletter. Second, we may rely on the performance of a contract under Article 6(1)(b), where processing is necessary in order to enter into or fulfil our contractual obligations to you, such as the provision of an enrolled course, the delivery of learning materials, the issuing of a certificate of completion, or the administration of assessments. Third, we may rely on compliance with a legal obligation under Article 6(1)(c), where processing is required by Irish or European Union law, including obligations relating to taxation, accreditation reporting, anti-money laundering, and child protection where applicable. Finally, we may rely on legitimate interests under Article 6(1)(f), provided that such interests are not overridden by your fundamental rights and freedoms; this basis is most commonly used for administrative, security, course-improvement, and quality-assurance purposes (Data Protection Commission [DPC], 2024).

3.2 Sensitive Information Disclosed in Learning Contexts

Although our educational services do not require us to process special category data as a matter of course, we recognise that learners on counselling, psychotherapy, and related courses may from time to time disclose information of a personal or sensitive nature in reflective assignments, discussion forums, or correspondence with tutors. Where any such information falls within the special categories listed in Article 9 of the GDPR, we process it only on the basis of explicit consent under Article 9(2)(a), or on another lawful basis recognised by Article 9, and we apply enhanced

confidentiality safeguards to such material. Learners are encouraged to limit personal disclosures in coursework to that which is necessary for the educational purpose at hand.

4. Categories of Personal Data We Collect

We endeavour to collect only such personal data as is necessary, relevant, and proportionate to the educational purposes for which it is processed, in keeping with the data minimisation principle in Article 5(1)(c) of the GDPR. The categories of personal data we may collect are described below.



4.1 Identification and Contact Data

We collect identifying information including your full name, date of birth, residential or postal address, email address, telephone number(s), and, where relevant, the name and contact details of an emergency contact or a sponsoring organisation. This information is necessary for the administration of your enrolment, the issuing of certificates, and to enable us to communicate with you in connection with your studies.

4.2 Academic and Course Data

For enrolled learners, we collect and maintain academic records associated with your participation on a course. These may include information about prior qualifications and relevant learning history, the courses for which you have enrolled, attendance and engagement records, submitted assignments and assessments, tutor feedback, marks and grades, certificates and awards issued, and any reasonable accommodations agreed in connection with assessment or learning support (QQI, 2022).

4.3 Administrative, Financial, and Technical Data



We collect enrolment scheduling information, fee and billing information, payment-card or electronic-transfer data (processed by accredited third-party payment processors and not retained on our own systems), correspondence relating to bursaries or instalment arrangements, and limited non-identifiable technical data generated by your interaction with our website and online learning environment, such as anonymised usage analytics and cookie data.

5. How Personal Data Is Collected

Personal data is collected through a number of channels, including the website enquiry, booking, and enrolment forms hosted on www.icps.ie; SSL-secured online booking and payment systems; intake and registration forms completed at the commencement of a course; the online learning environment and virtual classroom platforms used to deliver live and recorded sessions; in-person interactions where applicable; and ongoing email, telephone, video, and written correspondence between you and our administrative or academic staff. Wherever practicable, personal data is collected directly from you. Where information is provided by a third party, such as a sponsoring employer, professional body, or referee, we accept such information only with your prior consent or where the disclosure is permitted or required by law.

6. Online Bookings and Website Security

All online bookings, enquiry submissions, enrolments, and payments made through our website are protected by Secure Socket Layer (SSL) and Transport Layer Security (TLS) encryption protocols. This ensures that data transmitted between your browser and our servers is encrypted in transit and is not readable by unauthorised third parties. We implement and maintain reasonable technical and organisational measures, including firewalls,

anti-malware controls, regular software updates, access controls, and monitoring, to maintain the security and integrity of our website, online learning environment, and associated infrastructure (National Cyber Security Centre [NCSC], 2022). Nevertheless, no internet-based system can be guaranteed to be completely secure, and we encourage you to use a private and trusted device and connection when interacting with our online services.

7. Online Learning and Virtual Classroom Services

7.1 Secure Learning Platforms

Live online classes, recorded lectures, and asynchronous learning activities are delivered via learning management systems and virtual classroom platforms that have been selected for their suitability for educational delivery and their compliance with the security and data-protection requirements of the GDPR. Such platforms typically employ encryption in transit, access controls, multi-factor authentication, and other industry-standard safeguards. We maintain Data Processing Agreements with our online learning platform providers in accordance with Article 28 of the GDPR (European Parliament and Council, 2016).

7.2 Risks of Electronic Communication

While we take all reasonable precautions to safeguard your privacy during online learning activities, you acknowledge that no electronic communication system can be entirely free from risk. Risks include, but are not limited to, the possibility of interception by third parties, technical failures, and inadvertent disclosure caused by the involvement of multiple devices, networks, and service providers. By participating in our online learning activities, you

confirm that you have been informed of these inherent risks and that you accept them as a condition of participating in online courses.



7.3 Learner Responsibilities

To support the integrity and confidentiality of your learning experience, you are advised to attend live online classes from a private and quiet location where you cannot be overheard or interrupted; to use a personal device that is protected by a strong password or biometric lock; to ensure that the device's operating system, browser, and security software are regularly updated; to avoid public or unsecured Wi-Fi networks where reasonably possible; and to keep your login credentials, meeting links, and access codes confidential. We ask that learners do not record live sessions, screenshots, or other classroom material without the express written consent of the tutor and any other participants in the session.

8. In-Person Educational Activities

For learners attending in-person classes, workshops, or assessment events, personal data may be collected verbally during registration or by means of written or electronic forms. Any physical records, such as paper attendance sheets, signed enrolment forms, completed examination scripts, or printed correspondence, are stored securely in locked cabinets within premises to which access is restricted to authorised staff only. Classrooms, reception areas, and waiting facilities are arranged so as to protect learner confidentiality, and conversations involving identifiable academic information are conducted only in private settings.

9. Purposes of Processing



We process personal data for a defined and limited set of educational purposes, in keeping with the purpose-limitation principle of Article 5(1)(b) of the GDPR. These purposes include the provision of accredited diplomas, certificates, and continuing professional development programmes; the administration of enrolment, attendance, and assessment; the issuing of awards, transcripts, and certificates; communication with learners regarding course content, scheduling, and changes; the maintenance of accurate academic records to support quality assurance and continuity of study; billing, accounting, and financial administration; the management and improvement of our courses and the production of anonymised statistical analyses; the resolution of complaints and the handling of accreditation, insurance, or regulatory enquiries; and compliance with applicable legal, regulatory, and accreditation obligations. We do not process personal data for purposes incompatible with those for which it was originally collected, and we do not engage in automated decision-making producing legal or similarly significant effects within the meaning of Article 22 of the GDPR.

10. Confidentiality and Disclosure

All information disclosed to ICPS in the course of educational engagement is treated as confidential. Personal data, and in particular academic records and any sensitive material that may be shared in the course of reflective learning, will not be disclosed to third parties except in clearly defined circumstances. These include disclosures made with your explicit, informed, and freely given consent; disclosures to accreditation bodies, awarding bodies, or external examiners where such disclosure is necessary for quality assurance and certification; disclosures required or permitted by Irish or European Union law, including statutory reporting obligations relating to the protection of children and vulnerable adults under the Children First Act 2015 (Government of Ireland, 2015); disclosures necessary to prevent a serious and

imminent risk to the life or safety of yourself or another person; and disclosures made in response to a lawful court order, subpoena, or other valid legal instrument. In all cases, we disclose only the minimum information necessary to fulfil the relevant purpose, and where practicable we will inform you in advance of any disclosure that we propose to make.

11. Data Storage, Security, and Retention

11.1 Electronic Records

Electronic records are stored on secure systems that are protected by strong passwords, role-based access controls, encryption at rest where appropriate, and regular backup procedures. Access to learner records is restricted to those members of staff who require such access in order to perform their administrative or academic duties. Audit logs are maintained where technically feasible to enable the monitoring of access and the detection of any unauthorised activity (NCSC, 2022).

11.2 Physical Records

Any physical records, including handwritten notes, signed enrolment forms, examination scripts, and printed correspondence, are stored in lockable cabinets within secure premises. Such records are not removed from the premises except where necessary in the course of educational delivery, and they are transported in a manner designed to protect confidentiality.

11.3 Data Retention

Personal data is retained only for as long as is necessary to fulfil the educational purposes for which it was collected, taking into account applicable legal, accreditation, and regulatory requirements. The retention of academic records is informed by guidance issued by Quality and



Qualifications Ireland (QQI, 2022), the Higher Education Authority (HEA, 2023), and the requirements of our awarding partners and indemnity insurers. As a general rule, core academic records demonstrating that an award was made (including enrolment details, marks, and certificates issued) are retained on a long-term basis to enable verification of qualifications, while routine administrative correspondence is retained for shorter periods. Upon expiry of the relevant retention period, records are securely destroyed by means appropriate to the medium, including cross-cut shredding for paper records and secure deletion or physical destruction for electronic media.

12. Data Breach Management

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, we will take immediate steps to investigate, contain, and mitigate the breach. Where the breach meets the threshold set out in Article 33 of the GDPR, we will notify the Data Protection Commission of Ireland without undue delay and, where feasible, within seventy-two hours of becoming aware of the breach (DPC, 2024). Where the breach is likely to result in a high risk to your rights and freedoms, as set out in Article 34, we will also notify you directly without undue delay, providing clear information about the nature of the breach, the likely consequences, the measures taken or proposed to be taken, and the contact details of our data protection point of contact. We maintain an internal register of all personal data breaches, whether or not they are notifiable, in order to support continual improvement and accountability.

13. Your Rights Under the GDPR

The GDPR provides you with a robust set of rights in relation to your personal data. These rights include the right of access under Article 15, which





entitles you to obtain confirmation as to whether we are processing your personal data and, if so, to receive a copy of that data together with prescribed supplementary information; the right to rectification under Article 16, which entitles you to have inaccurate personal data corrected and incomplete data completed; the right to erasure under Article 17, also known as the “right to be forgotten,” which entitles you to request the deletion of your personal data in certain circumstances; the right to restriction of processing under Article 18, which enables you to limit the way in which we use your data in defined situations; the right to data portability under Article 20, which entitles you to receive your data in a structured, commonly used, and machine-readable format and to have it transmitted to another controller where technically feasible; the right to object under Article 21, including the right to object to processing based on legitimate interests; and the right to withdraw consent at any time under Article 7, where consent is the lawful basis for processing, without affecting the lawfulness of processing carried out before withdrawal (European Parliament and Council, 2016).

Requests to exercise any of these rights should be made in writing to GDPR@icps.ie. We will respond to all valid requests within the statutory timeframe of one calendar month, which may be extended by a further two months where necessary, taking into account the complexity and number of requests. We may need to verify your identity before responding to a request in order to protect against unauthorised disclosure. There is generally no fee for exercising your rights, although we may charge a reasonable fee, or refuse to act, where a request is manifestly unfounded or excessive (DPC, 2024).

14. Cookies and Website Analytics

Our website may use cookies, pixel tags, and similar tracking technologies in order to ensure the proper functioning of the site, to remember your



preferences, and to gather aggregated, non-identifiable information about how the site is used so that we can improve performance and user experience. Strictly necessary cookies are deployed without your consent, in accordance with the ePrivacy Regulations (S.I. No. 336 of 2011) and DPC guidance, while non-essential cookies, including analytics and marketing cookies, are deployed only where you have provided your consent through our cookie banner (DPC, 2020). You may withdraw or modify your consent at any time, and you may also disable cookies through your browser settings, although doing so may affect the functionality of certain features of the website and online learning environment.

15. Third-Party Processors and International Transfers

We may engage carefully selected third-party service providers to process personal data on our behalf, including providers of online booking and enrolment systems, learning management systems, virtual classroom platforms, payment processing, email and communication services, accounting software, and IT support. All such processors are subject to written Data Processing Agreements that meet the requirements of Article 28 of the GDPR, and they are required to implement appropriate technical and organisational measures and to process personal data only in accordance with our documented instructions (European Parliament and Council, 2016). Where any transfer of personal data to a country outside the European Economic Area is contemplated, we ensure that an appropriate transfer mechanism is in place, such as an adequacy decision of the European Commission, the use of Standard Contractual Clauses, or another lawful safeguard recognised under Chapter V of the GDPR.

16. Complaints and Supervisory Authority

If you have any concerns about the way in which your personal data is being handled, we encourage you to contact us in the first instance at GDPR@icps.ie, so that we may have the opportunity to address your concerns directly. You also have the right, at any time, to lodge a complaint with the Irish Data Protection Commission, which is the independent supervisory authority responsible for monitoring the application of the GDPR and the Data Protection Act 2018 in Ireland. The Commission may be contacted at 21 Fitzwilliam Square South, Dublin 2, D02 RD28, by telephone on +353 (0)1 765 0100 or 1800 437 737, or via its website at www.dataprotection.ie (DPC, 2024). Complaints concerning academic matters may also be addressed in line with the Institute's published academic complaints procedure.

17. Changes to This Privacy Policy

This Privacy Policy is subject to periodic review and may be updated from time to time in order to reflect changes in our practices, in technology, in applicable law, or in regulatory and accreditation guidance. The most current version of the Policy will always be available on our website at www.icps.ie, and the "Last Updated" date at the top of the Policy will be amended accordingly. Where changes are material, we will take reasonable steps to bring them to your attention, for example by means of a notice on our website or, where appropriate, by direct communication. Your continued use of our educational services following the publication of an updated Policy constitutes acknowledgement of the changes.

References

- Bond, T. (2015). *Standards and ethics for counselling in action* (4th ed.). Sage Publications.
- Data Protection Commission. (2020). *Guidance note on cookies and other tracking technologies*. Data Protection Commission. <https://www.dataprotection.ie>
- Data Protection Commission. (2024). *A guide to your rights – Plain English guide to data protection*. Data Protection Commission. <https://www.dataprotection.ie>
- Department of Education. (2022). *Statement of strategy 2023–2025*. Government of Ireland.
- European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.
- Government of Ireland. (2015). *Children First Act 2015*. The Stationery Office.
- Government of Ireland. (2018). *Data Protection Act 2018*. The Stationery Office.
- Higher Education Authority. (2023). *Statement of strategy 2023–2027*. Higher Education Authority.
- Information Commissioner’s Office. (2023). *Guide to the UK General Data Protection Regulation*. ICO. <https://ico.org.uk>



National Cyber Security Centre. (2022). *Cyber security baseline standards for public service bodies*. NCSC Ireland.

Quality and Qualifications Ireland. (2022). *Core statutory quality assurance guidelines*. QQI.

S.I. No. 336/2011. (2011). *European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011*. The Stationery Office.