



## Data Protection & Privacy Policy

---

Effective from 25 May 2018

*All Insurance Institute examinations are now delivered in an online proctored environment, unless stated otherwise. For this purpose, technology services are delivered by a third party, TestReach Ltd, which will invigilate the examinations and collate the results of multiple choice questions. Please see the Addendum to the Data Protection and Privacy Policy below [\[directly accessible here\]](#) which explains the use and management of personal data in this context.*

The Insurance Institute, a professional educational body dedicated to providing education and training to insurance professionals, is committed to protecting your privacy and the security of your data. Any personal information you disclose to us will be treated with the highest standards of security and confidentiality in accordance with applicable Data Protection Laws. Please read the following statement carefully, it sets out how we process and protect your personal information and your rights in relation to your data.

In this statement we use the terms “we” and “our” to refer to the Insurance Institute.

### 1. What is personal data?

Personal data is any information relating to an identified or identifiable living person. We collect information, including personal information on our members, students, apprentices, prospective members, students and apprentices, users of our website and online services, engagers with our social media channels, attendees at our events and others. In this capacity, we are the controller responsible for your personal data.

### 2. How we collect personal information

We collect personal information directly from you when you register for membership or for exams, when you accept designations, use our CPD scheme, enrol for apprenticeships, contact member services, use our website and update your account, engage with our social media channels, attend events, make payments for services or goods and/or make enquiries or complaints.

We use an online membership system to manage student membership, enrolment, and academic records. This information is used to maintain accurate student data, support teaching and administration, issue communications, comply with educational and legal requirements, and enhance the overall student experience.

We also collect your personal information when you engage with online services that we use to provide academic training or webinar for our members e.g. e-learning/LMS platform. This information is used to provide access to courses, verify identity, record participation, deliver and assess learning, monitor academic progress, issue communication, comply with educational regulations, improve the learning experience and ensure security. Access to this data is limited to instructors, authorised administrators, and approved educational tools or integrations. Data is retained in line with academic and legal requirements, and students may request access, correction, or deletion of their data where applicable.

We may also collect information indirectly from our educational partners, your employer (e.g. to verify your identity if they are funding your membership or exams), other regulatory bodies (e.g. CII if you are a dual member) or public sources (e.g. media reports).

### **3. What personal information do we collect from you?**

The personal details we collect from you include the following:

- Name, home address, email address, phone number(s)
- Title
- Date of Birth
- Maiden name
- Gender
- Employer's name, address and contact details
- Employment details e.g. area of work, job title
- Member ID number
- Qualifications
- Exam attendance, results and designations
- CPD details
- Nationality, Country of Birth, PPS No. [Required by ATU Sligo, our current awarding body]
- Bank account details/Credit Card details
- Course activity data including assignments, submissions, quizzes, grades, feedback, attendance, entry/exit logs
- Learning progress information such as completion tracking, time spent on activities, and overall performance
- Technical and usage data such as login times, device/browser type, and IP addresses for security and system functionality.

Members are obliged to provide this information to us for the purposes of the membership contract. If you do not provide us with this information we cannot perform the contract with you.

In certain, limited circumstances, we may also collect special category/sensitive data (e.g. medical certificates supplied for the purposes of deferring an exam; applications for pro-rata CPD). When we collect sensitive information about you, we do so with your consent, we explain why we need the information, what it is used for and you can withdraw your consent by contacting us.

We may also collect information through the use of cookies on our website and other technology which collects (non-personal) analytical information relating to visitors to the website as set out in more detail in the [Cookies Notice](#) (available on our website). We use this information to monitor traffic and to improve your experience of the website.

We may invite users to participate in optional anonymous surveys. These surveys do not collect personal data.

### **4. How do we use your information?**

We may use your personal information in the following ways:

- To manage and administer your membership with the Institute

- To maintain details of qualifications, accreditations and designations
- To provide a CPD scheme and maintain CPD records
- To organise events, lectures, workshops
- To provide details of training courses and study materials
- To provide learning support and feedback
- To hold exams, maintain exam records & provide additional educational supports
- To provide industry news and updates
- To respond to your queries, complaints and provide service support
- To provide member bonuses e.g. discounts on goods or services
- To fulfil our disciplinary, statutory and regulatory functions
- For marketing purposes to include surveys and statistical analysis
- To enhance and improve our services
- To collect fees

## **5. Lawful basis for collecting your personal data**

We use the personal data where necessary for the following lawful purposes:

1. To enter into and perform our contract with you e.g. to register you for membership, for exams or to award designations.
2. Where we have a legitimate interest or it is in the legitimate interests of a third party e.g. in order to run our business, sharing data with your employer.
3. Where there is a legal, statutory or regulatory requirement to do so (e.g. Maintaining a Register of Compliant Persons under the Central Bank's Minimum Competency Code 2017).
4. Where you have consented to the use of your data (e.g. request for special assistance during an exam).
5. To protect the vital interests of you or others (e.g. in emergency situations) or
6. It is in the public interest.

## **Marketing Communications**

The Institute may direct information relating to topics, goods or services to you which we feel will be of interest to you. You have options as to what marketing emails to receive or not to receive and you can manage these at any time through our online Preference Centre.

## **6. Your information and third parties**

We sometimes share your information with third parties.

For example we share your information with:

- educational partners (e.g. CII, IOB, LIA, HEA, SOLAS) and awarding body (ATU Sligo)
- your employer where they are sponsoring your membership, exams or CPD
- our service providers (e.g. cloud-based services, Canvas Credentials, Turnitin)
- the Central Bank, if requested, to facilitate them in discharging their functions under their Minimum Competency Code (MCC)
- Our Local Institutes when you attend a Local Institute event or initiative

- law enforcement or other authorities if required by applicable law
- in the event of a merger or proposed merger.

We never sell your information to a third party.

## **7. How long your personal information will be kept for**

Information will be retained for no longer than is necessary for the purpose for which it was obtained by us or as required by legal and regulatory purposes and for legitimate business purposes.

Where your membership has lapsed for a significant period we will delete the majority of your personal data we hold, but will maintain your academic record with us (if any), your CPD record (for MCC purposes) and a minimum amount of basic personal data to ensure that we do not inadvertently create a new record in the system.

Exam scripts will only be retained for the period during which an appeal may be lodged plus one month, or if an appeal is lodged, for a month after the end of the appeal process.

Coursework assignments will only be retained for the period during which an appeal may be lodged plus one month, or if an appeal is lodged, for a month after the end of the appeal process. However the assignments will also be uploaded onto Turnitin anti-plagiarism software and securely stored on Turnitin's database for comparative purposes.

## **8. Keeping your personal information secure**

We have appropriate technical and organisational security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. These measures include IT security (encryption, firewalls), staff training and awareness, office and building security and limiting of access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

Although we take all appropriate steps to safeguard your data, no website, device, wifi connection or system can ever be completely secure.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

## **9. Disclosures of Personal data outside of the EEA**

We will not ordinarily transfer Personal Data to countries outside the European Economic Area (EEA) (unless, for example, we are corresponding with a Member who resides outside of the EEA). If any data is processed outside of the European Economic Area (EEA), we will ensure there are measures in place in association with the processor to ensure this is consistent with GDPR. We will comply with the obligations under data protection legislation to ensure such transfers are lawful.

## **10. Your rights**

Under Data Protection law you have a number of important rights. In summary, those rights include the right to:

1. Access your data – you can request details of the personal information which we hold about you and receive copies.
2. Request rectification – you can have any mistakes in your information which we hold corrected.
3. Be forgotten – you can have the personal information concerning you deleted in certain situations.
4. Data Portability – i.e. obtain a transferable copy of your information we hold to transfer to another provider.
5. Withdraw Consent – where we are relying on your consent to process your data, you have the right to change your mind and withdraw consent by contacting us.
6. Object to processing – you have the right to object to specific types of processing of your personal data (e.g. direct marketing).
7. Rights relating to automated decision making including profiling – you have the right in respect of automated decision making, including profiling. Where we carry out solely automated decision making, including profiling, which has legal or similarly significant effects on you, we can only do this if it is in connection with a contract with you, we have a right under law or you have provided your explicit consent.
8. Restrict Processing – you have the right in certain specified situations to require us to stop processing your information and only store it.

If you would like to exercise any of these rights, free of charge, please contact us in writing as set out below. We will respond without undue delay and no later than one month from receipt of any such request. If we are unable to deal with your request within a calendar month (due to complexity or number of requests) we may extend this period by a further two calendar months and will explain the reason why.

**Please note that we will request proof of your identity and address (e.g. a copy of your driving licence or passport) to protect the security of your data.**

## **11. How to complain**

If you have a complaint about the use of your personal information, please let us know. We will try to resolve any query or concern you raise with us.

The General Data Protection Regulation also gives you right to lodge a complaint with a supervisory authority. The supervisory authority in Ireland is:

**The Data Protection Commission, 6 Pembroke Row, Dublin 2, D02 X963.  
Email: [info@dataprotection.ie](mailto:info@dataprotection.ie)**

**Phone: Mon – Fri: 9.30am – 1pm : 01 765 0100 / 2pm to 5pm : 1800 437 737**

## **12. How to contact us**

Please contact us if you have any questions about this privacy notice or the information we hold about you. If you wish to contact us please send an email to [dataprotection@iii.ie](mailto:dataprotection@iii.ie) or write to ***The Secretary, The Insurance Institute, 5 Harbourmaster Place, IFSC, Dublin 1.***

**Updates to this privacy notice**

This privacy notice is effective from 25 May 2018. We may change this privacy notice from time to time. If there are material changes we will notify you either by posting on the website or by other communications.

Last updated: 19th December 2025