

Privacy and Data Protection Policy

This policy explains how GC Academy Limited uses personal information in connection with your IJF Academy application, studies and academic records, and how you can exercise your privacy rights. It covers the learning platform, assessment, practical learning and related communication, including records retained after you leave.

Who is responsible for your information

GC Academy Limited, company registration number **C72007**, is the data controller for the processing described in this policy. “We” and “us” mean GC Academy Limited. IJF Academy is the educational service to which this notice relates.

Registered office: Apartment 4, Villanueva Building, 99, Hanneqa Street, Ghaxaq GXQ1025, Malta.

Privacy contact: academy@ijf.org. Please identify your message as “Privacy – GC Academy / IJF Academy”. You may also write to the registered office. You do not need to approach a tutor or your federation first.

Information used for your studies

- **Application and account details:** your name, personal email and contact details, nationality, relevant identity and qualification evidence, federation nomination, account credentials and agreements.
- **Learning and assessment records:** enrolment, platform activity, attendance, assignments, forum contributions, test responses, marks, feedback, practical evidence, certificates and relevant identity-check images.
- **Support and administration:** correspondence, complaints or appeals, information needed for requested support, fee or sponsorship references, technical and security logs, and consent choices where relevant.

We receive information from you and your platform use, and where relevant from tutors, assessors, your nominating federation or sponsor, and sources used to verify your identity or qualifications. We use only information relevant to the stated purpose.

Why your information is needed

Information is used to register and support you, provide learning and assessment, communicate about your studies, record progress, issue and verify awards, protect examination integrity and platform security, resolve concerns, improve educational provision and meet applicable legal or accreditation requirements.

Required information and the effect of not providing it must be explained when it is requested. Without information needed to verify eligibility or identity, we may be unable to register you or provide the relevant assessment. Optional publicity or marketing choices do not determine your academic treatment.

Legal grounds and identity checks

The legal grounds for using your data

The EU General Data Protection Regulation (GDPR) and Malta's Data Protection Act govern this processing. A legal ground must apply to each use of your information.

- **Legitimate interests:** administering your requested education, keeping reliable academic records, protecting assessment integrity and security, improving the service and handling concerns. These interests must be balanced against your rights; you may object as explained below.
- **Contract:** processing necessary for a contract you enter into directly with GC Academy Limited, or steps you request before that contract. A contract with another organisation does not by itself establish this ground for GC Academy.
- **Legal obligation:** records or disclosures required by a legal duty binding on GC Academy Limited. This applies only where such a duty exists.
- **Consent:** optional uses such as publicity, promotional messages or non-essential tracking where consent is required. Consent must be specific and freely given and can be withdrawn. Enrolment, platform use or camera permission is not blanket consent to other uses.

Health information and other sensitive data

Provide health or disability information only where needed for support, safety or an adjustment, through a private channel. Access must be limited to people who need it; a tutor generally needs the agreed arrangement rather than your full medical history.

Health data and biometric data used to uniquely identify you require an additional lawful condition under GDPR Article 9. Before collection, you must be told the purpose, the applicable legal grounds, who will receive the data and how long it will be retained. Explicit consent can be used only where it is genuinely freely given.

Facial identity checks and automated functions

For examinations using facial recognition, the Handbook describes a comparison between your sign-up reference photograph and a camera image at the start of the test through Microsoft Azure. The test opens after a successful match. If the match fails, the Handbook permits a new reference photograph; this failed check does not use the first examination attempt where the Handbook expressly provides this protection.

The platform also scores online tests and monitors progress against programme requirements. These functions can restrict further attempts or course access under the Handbook. This policy does not change those academic rules. Contact the Academy if a technical error or an incorrect record affects you; the complaint and appeal route is on the final page.

A photograph is not automatically special-category data, but biometric processing for unique identification is. The Handbook's description does not replace the specific privacy information and lawful grounds required for that processing. You may ask about the images or biometric information used, storage, recipients and available support before an examination.

Sharing storage and protection

Who can receive your information

Only information needed for a lawful, stated purpose may be shared with:

- Authorised IJF Academy teaching, assessment and support personnel, and providers of hosting, platform maintenance, communications and approved learning services, including Microsoft Azure for the Handbook's facial identity checks.
- Your nominating federation or sponsor for relevant nomination, participation, sponsorship or completion information. This does not give them unrestricted access to health information, private correspondence or complaints.
- Accreditation bodies, regulators, auditors, professional advisers or competent authorities where disclosure is necessary and lawful.

Forum contributions are visible to the relevant participants. Keep health, identity and complaint information private. Respect others' privacy and obtain the necessary permissions for project material or recordings. Assessment submissions do not themselves authorise unrelated public promotion.

Processing outside the European Economic Area

Hosting, support and authorised access may involve different countries. Transfers outside the European Economic Area require a valid GDPR mechanism, such as an applicable adequacy decision or approved contractual safeguards with any necessary additional protection. Registration is not blanket consent to international transfers.

You must be informed of applicable transfers and safeguards. Contact us for the relevant destinations, recipients and information about obtaining a copy of the safeguards.

How long information is kept

Retention depends on the purpose and the applicable legal or accreditation requirements:

- **Academic records and awards:** retained to preserve the required academic archive and verify your achievements. Leaving a course or closing an account does not automatically erase these records.
- **Identity evidence and examination images:** limited to the verification purpose and any necessary review, appeal or justified legal claim. They do not automatically share the retention period of your certificate or academic transcript.
- **Support, case, financial and technical records:** kept for the relevant support or case purpose, necessary legal claims, applicable financial duties or justified security need. Optional material follows its stated purpose and consent arrangements.

Information no longer needed must be deleted or effectively anonymised. You may ask which criteria apply to your records. Handbook programme limits and expiry of results do not themselves set personal-data deletion dates.

Keeping information secure

Access must be restricted and information protected against loss, misuse or unauthorised disclosure. Protect your password and report suspected account misuse, lost records or misdirected messages to academy@ijf.org. If a breach creates a high risk to you, you must be informed where the GDPR requires it.

Your rights and getting help

Your data protection rights

Depending on the GDPR conditions, you may:

- **Access and correct** your personal data, obtain a copy and ask for inaccurate or incomplete details to be corrected.
- **Request erasure or restriction** where the legal conditions apply. Necessary lawful records or legal claims may justify retaining some information.
- **Receive portable data** you supplied where automated processing is based on consent or contract, in a structured, commonly used, machine-readable format, with direct transfer where technically feasible.
- **Object to legitimate-interest processing** on grounds relating to your situation. It must stop unless overriding compelling grounds or legal claims justify continuation. Direct marketing objections must be honoured without requiring a reason.
- **Withdraw consent** at any time, without affecting earlier lawful processing. Refusing or withdrawing optional publicity or marketing consent must not disadvantage your studies.
- **Exercise safeguards for automated decisions** with legal or similarly significant effects, including human intervention and contesting a decision where the GDPR provides these rights.

Making a privacy request

Write to academy@ijf.org or the registered office given on the first page. Describe your request and provide enough information to locate your records. No special form or legal wording is required. If there is reasonable doubt about your identity, we may request only the additional information needed to verify it.

Requests are normally free. We must respond without undue delay within the periods required by the GDPR. Any permitted extension, restriction, fee or refusal must meet the GDPR conditions and be explained, including the available remedies. This policy does not replace those statutory rights or periods.

Privacy complaints and academic appeals

You may complain directly to Malta's [Information and Data Protection Commissioner](#) or another competent data protection authority, including where you live or work or where the alleged infringement occurred. You do not need Academy permission or a completed academic appeal. Judicial remedies remain available.

For an academic complaint or appeal, follow the Student Handbook: use the Academy's **Contact Us** form, select "**Complain**" or "**Appeal**", and provide a detailed description. The Head of Institution communicates the final appeal decision. Correcting personal data and challenging an academic judgment are distinct requests; you may raise both where relevant.

Cookies and changes to this notice

Essential cookies support functions such as sign-in and security. Non-essential tracking requires prior consent where applicable, with a way to refuse or withdraw it. You must be told the relevant cookie purposes and durations. Material changes to the use of your information must be explained; updating a notice does not create retrospective consent.

[Student Handbook](#) | [Contact Us](#) | [GDPR rights and response rules](#)