



INSTITUTE OF PROJECT PROFESSIONALS

Privacy Notice and Data Protection Policy

What we hold about you, why, who can see it, and how long we keep it



This is both the privacy notice we give to the people whose personal data we hold, and the policy we work to. It is one document rather than two because a notice that says something different from the policy behind it is a notice nobody has checked.

It is written from the running platform. Every statement below about what is held, who can see it, and what happens when you ask for it to go describes what the live system actually does, not what it is intended to do.

This document replaces the privacy policy published at ipp.pro/privacy on 4 July 2026. The page at that address is generated from this document, so the two cannot disagree.

1. Who we are

Module Six Ltd is the data controller for your personal data, and is registered in England and Wales under company number 17311940. Its registered office is Henge Barn, Pury Hill Business Park, Alderton Road, Towcester, Northamptonshire, NN12 7LS. It is registered with the Information Commissioner's Office under reference **ZC198668**.

The Institute of Project Professionals is operated by Module Six Ltd. It is not a separate legal entity, so where this document says IPP decides something it means Module Six Ltd acting as the Institute, and Module Six Ltd is answerable for it.

1.1 The platforms this covers

Platform	What it is
ipp.pro	Membership, applications, qualifications, the public directory and credential verification
activate.modulesix.io	Learning and examinations
calibrate.modulesix.io	The competency record, CPD and the Passport
educate.modulesix.io	Open courses and Certificates of Achievement
validate.modulesix.io	Authority to Work. See Section 1.2, the controller is different
candidate.modulesix.io	Verified talent and the agency window
business.modulesix.io and shop.modulesix.io	Organisation purchasing and licensing
explore.modulesix.io	The front door to the ecosystem. Reads your Passport to show you where you already are
id.modulesix.io	Shared sign-in across the platforms above

1.2 Authority to Work is different

Validate holds competence, authorisation and evidence records about named workers so that an employer can show who is cleared to do what. For those records the **employer is the controller and Module Six Ltd is the processor**. Many of the people in them have no IPP account and never asked us for anything.

This matters to you in one practical way. If you ask us to erase you and you also appear in an employer's Authority to Work records, we will show you everything held and pass your request to that employer, but we will not delete their competence records on the instruction of somebody



who is not their controller. Doing so would destroy an employer's evidence that its people were qualified to do the work they did.

1.3 How to reach us

Email **data@ipp.pro** for anything in this document, including exercising any right in Section 7. You do not need a particular form of words and you do not need to say which right you are using. Say what you want and it will be routed. We respond within one month.

A complaint about how a request was handled goes to governance@ipp.pro under IPP-GOV-006, which is the single intake for every complaint. That is a different address for a different purpose, and using the wrong one will not cost you anything: either is passed on.

2. What this document owns

Every other document in the estate that touches personal data points here rather than restating any of it.

This document owns	Where
The controller, and the two controller relationships	Sections 1.1 and 1.2
Lawful basis for every purpose	Section 3
Who can see what, including employers and the public	Section 5
The retention schedule, including backups	Section 6
Your rights and how a request is handled	Section 7
Processors, and where your data goes	Section 8
Security, breaches, cookies and minimum age	Sections 9 to 11

- **What appears on a public surface, field by field**, is IPP-DAT-002, issued 10 August 2026. Section 5.6 states the principle and the lawful basis; DAT-002 states the field, the label a reader sees, and what a reader may conclude from it.
- **How to complain** is IPP-GOV-006.
- **Examination conduct, adjustments and malpractice** is IPP-ASM-002. This document owns the retention and disclosure of the records those create.
- **What you may claim about your membership** is IPP-GOV-005.

Nothing here limits your statutory rights, and nothing requires you to use our process before going to the Information Commissioner's Office. Section 7.6 says how.

3. What we hold, why, and on what basis

Every category below exists in the live platform. Where the basis is consent it means a choice you actually made and can take back, not an inference from your continuing to use the service. The last two columns make this table the record of processing activities we are required to keep, so you are reading the same record a regulator would. Section 6 gives the retention rules in full and wins where the summary here is shorter.



Category	What it includes	Purpose	Lawful basis	Kept for	Who sees it
Account and identity	Name, email address, sign-in sessions and the browser they were opened in	Letting you in, keeping you in, keeping other people out	Contract	While your account is open	Us, Clerk
Membership	Grade, member number, status and its history, applications and their evidence, endorser names and addresses, checkout consents	Admitting, renewing, suspending and reinstating membership	Contract. Legal obligation for the consent record	Account: while open. Consents: six years	Us, Clerk
Payment	Billing identifiers, subscriptions, quotes, concessions, discounts and redemptions	Taking payment and keeping the accounting record	Contract. Legal obligation for the financial record	Six years from the end of the financial year	Us, Stripe
Concession evidence	Evidence of student or military status	Deciding a reduced fee	Contract	Deleted at the decision	Us
Assessment	Sittings, the questions drawn, the answers given, scores, passes, certificates and references, resits and appeals	Awarding and verifying a qualification	Contract	While your account is open	Us
Reasonable adjustments	What was asked for, what evidence was seen, what was agreed, by whom, until when	Making an assessment accessible	Contract. Legal obligation under equality law	While your account is open	Us
Competency record	Self-assessments, validated levels and their history, evidence entries, reviews and notes, development plans	The professional record the whole service exists to build	Contract	While your account is open	Us, your reviewer, your employer where you hold their seat
CPD	Activities, hours, reflections, and whether an entry is marked private	Renewal compliance and your own development record	Contract	While your account is open	Us, your reviewer, your employer unless marked private
Endorsements	Delivery claims, outcome statements, the people asked to verify them and what they said	Establishing that claimed work was actually done	Contract. Consent for the person asked to verify	While your account is open	Us, the verifiers you name, agencies if published
Multi-rater feedback	Requests, raters, scores and comments	Development feedback within an organisation	Contract	While your account is open	Us, your employer, the raters you name



Category	What it includes	Purpose	Lawful basis	Kept for	Who sees it
Deployments	That you were deployed, to which organisation, until when, and any concern raised about the work	Letting a host see validated competence while you work there	Consent, given when you accept the deployment	While your account is open	Us, your employer, the host organisation
Talent window	Availability, notice period, day rate range, sectors, travel	Being found by an agency	Consent, twice over: open to work, and published	While your account is open	Us, approved agencies
Public register entry	Your name, grade, designation and status in the member directory	Letting an employer or a client confirm you hold what you say you hold	Legitimate interests. Removable from your account at any time	While your account is open and the entry is on	Anyone
Directory profile and Passport	Job title, employer, location, biography, LinkedIn address, qualifications, competency summary and CPD position	Showing more than the credential, where you have asked us to	Consent. Off unless you turn it on	While your account is open and you leave it on	Anyone, or whoever holds your Passport link
Authority to Work	Competence holdings, authorisations, submissions, approvals and uploaded evidence	An employer showing who is cleared to work	Your employer's basis, not ours. See Section 1.2	As long as your employer requires	Your employer, us as their processor
Contact record	Which notifications we sent you and when. Not their content	Not sending you the same thing twice	Legitimate interests	While your account is open	Us, Resend
Technical data	IP address and request data, handled by our infrastructure provider as part of serving a page	Running the service and keeping it up	Legitimate interests	Held by Cloudflare on its own retention	Us, Cloudflare
Audit log	What was done to your record, by whom and when	Being able to show what we decided and why	Legal obligation and legitimate interests	Six years from the entry	Us

We do not hold special category data as a matter of course and we do not ask for it. A reasonable adjustment can be granted on evidence describing a barrier without naming a diagnosis, and IPP-ASM-002 Section 4 says so. Where a document you send contains more than was needed, it is read for the barrier it describes and deleted with the decision under Section 6.

We do not use your data for marketing without your explicit consent, and we send no promotional email unless you have opted in. We buy no personal data, enrich no record from a third-party source, and build no profile about you from anything other than what is listed above.

4. Where it comes from

- **From you**, when you create an account, apply, sit an assessment, record CPD, or fill in a profile.
- **From your employer**, where they hold a licence and have assigned you a seat, or where they operate Authority to Work.
- **From people you nominate**, when an endorser, verifier or rater responds to a request you started.

- **From your reviewer**, when a competency level is validated or a review is recorded.
- **From the platform itself**, when you sit a paper, are issued a certificate, or a renewal falls due.

5. Who can see it

The rule is that your professional record is yours. You build it, people you or your employer nominate validate it, and it travels with you when you change employer. Everything below is an exception, and each one is either something you switched on or something the service cannot work without.

5.1 Us

Staff see what they need for the task in front of them: membership and assessment decisions, application review, adjustment decisions, support, billing, and handling your own requests. Every staff view of a subject's full record is written to the audit log, including the export produced to answer a subject access request.

5.2 Reviewers and assessors

A reviewer sees the competency record, evidence and development plan of the people assigned to them, and CPD entries not marked private. They do not see examination attempts, payment records or applications.

5.3 Your employer, where you hold a seat they pay for

An organisation administrator sees competency levels both self-assessed and validated, evidence entries, CPD entries not marked private, development plans, and reviews. They do not see your examination attempts, your assessment answers, your reasonable adjustments, your payment records, your membership applications, or anything you marked private.

When you leave an organisation your record remains yours. It is not deleted and the organisation does not keep a copy.

Marking a CPD entry private means your employer cannot see it. Until 10 August 2026 that held for the team report and the reviewer view and did not hold for the organisation-wide report, which read every entry regardless. It is fixed, and it is recorded here rather than quietly, because members were told those entries were private and for a period they were not.

5.4 A host organisation, while you are deployed to them

A deployment does not start until you confirm it yourself. While it runs the host sees your name, your home organisation, your membership grade, the end date, and your **validated** competency levels at area level. They do not see self-assessed levels, element detail, evidence or CPD, and they cannot write to your competency record. Access ends automatically on the end date.

A host may raise a concern about the work, which goes to your home organisation and is recorded against your record. You may ask to see any concern raised about you under Section 7.

5.5 Agencies, through the talent window

An agency sees nothing until you have turned on both open to work and published. Then they see your name, grade, designation, verified delivery outcomes and the organisations you delivered at, and what you have stated about availability, rate and travel. They do not get your email address or any other contact route: an approach comes back through us.

5.6 The public

Three surfaces are reachable without signing in, and they behave differently.

- **The member register.** Your name, grade, designation and status. **A member with an allocated member number is listed by default**, because a credential nobody can check is not a credential, and you can remove your entry at any time from your account. Searchable by name only.
- **Your profile on that entry.** Job title, employer, location, biography and LinkedIn address. **Off unless you turn it on.** None of it is needed to confirm you are who you say you are, and it is a separate switch for that reason. Turning your listing off takes the profile with it.
- **Your Passport.** A shareable read-only page showing your grade, qualifications, competency summary and CPD position. **Off unless you turn it on.**
- **Certificate verification.** Anyone holding a certificate reference can confirm it is genuine and see the holder's name, the qualification, the date and the score. This exists so that a certificate can be checked by the person you gave it to.

The register is not searchable by employer. Looking up whether a named person holds a credential and listing everyone who works at a named company are different things, and only the first is what a register is for.

- The same split applies to the Passport. Your job title and employer are profile fields wherever they appear, so they are published on your Passport only where you have switched the profile on. Until 10 August 2026 the Passport published them regardless, which meant a choice you made for the register was not honoured on the page you were most likely to send somebody.

The field-by-field detail of all four, and the labels a viewer sees, is IPP-DAT-002. Where DAT-002 and this document appear to differ on a field, this document owns the basis and DAT-002 owns the field.

6. How long we keep it

Two things decide how long a record lives: whether your account is open, and whether it is something we have to be able to produce later. Nothing is kept because deleting it was never got round to.

Record	Kept	Then
Account, competency record, CPD, evidence, development plans, learning progress	While your account is open	Deleted when you close it or ask for erasure
Assessment sittings, answers, scores and certificates	While your account is open	Deleted with the account. A certificate already issued stays verifiable by reference until then
Reasonable adjustment records	While the adjustment is live, and while the account is open	Deleted with the account
Evidence uploaded with an application	Until the application is decided	Deleted at the decision, approved or refused. We keep the outcome, not the evidence
Concession and status evidence	Until the claim is decided	Deleted at the decision
The application record itself	While your account is open	Deleted with the account

Record	Kept	Then
Endorsements, feedback and deployment records	While your account is open	Deleted with the account
Payment and commercial records	Six years from the end of the financial year they fall in	Deleted. Kept through a closure, deleted on an erasure
Membership consent records	Six years from the end of the membership year they relate to	Deleted
Complaint, conduct and appeal records	Six years from the closure of the matter	Deleted
Audit log	Six years from the entry	Deleted
A closure or erasure request	Six years from the request	Deleted. This is the record that we did what you asked
Retired member numbers	Permanently	Never reused. A number and a date, no name attached
Sign-in sessions	Seven days idle, thirty days at the outside, eight hours on a shared device	Expire and are deleted
Daily database backups	30 days	Expire automatically
Weekly database backups	12 months	Expire automatically
Authority to Work records	As long as the employer requires	The employer decides. See Section 1.2

These periods are applied by a deletion that runs monthly, as well as when you close your account, ask for erasure, or a decision ends a record's purpose. A period nothing acts on is an intention, not a retention rule.

6.1 Backups, stated plainly

The database is copied nightly and weekly. Those copies are how the service survives a failure and cannot be edited: a backup you can reach into and alter is not a backup. So an erasure removes you from the live service immediately and from the backups as they expire, within 30 days for the daily copies and 12 months for the weekly ones. Nothing is restored from a backup without checking it against the erasure record first.

6.2 A lapsed membership is not a closed account

If a membership lapses, the designation and its benefits stop and the account returns to the free floor. Nothing is deleted, and your competency record, CPD log and qualifications remain yours and remain visible to you. Only a closure or an erasure deletes anything. Any earlier IPP material describing a fixed deletion period for lapsed members is superseded by this section.

7. Your rights

Exercise any of these by emailing data@ipp.pro. There is no fee and you will not be asked to justify the request.

Right	What it means here
Access	A copy of everything held about you, gathered from every part of the platform and given to you in a readable form
Rectification	Correcting anything wrong. A validated competency level is corrected through your reviewer, because the record has to show who validated what
Erasure	See 7.2. Two routes, and they do different things
Portability	Your record in a machine-readable form. It is designed to be portable: that is what the Passport is for
Restriction	Asking us to stop using a record while a disagreement about it is resolved
Objection	Objecting to a use that relies on legitimate interests
Withdrawing consent	Turning off the directory, the Passport, the talent window or a deployment. Immediate, and it does not affect anything done before

7.1 How to make one, and how long it takes

There is no self-service download. You email data@ipp.pro and we gather it: everything held about you, from every part of the platform, sent to you in a readable form. It is complete and it is inside a month, but it is not a button you press.

A request is answered within one month. Internally it is flagged at 21 days if it has not been dealt with, so the deadline is noticed before it is missed rather than after. If a request is genuinely complex and needs longer, you are told inside the month, told why, and told when to expect an answer.

7.2 Closing your account, and erasing it

These are different requests and you choose which one you are making.

- **Closure** means you are leaving. Your professional record, learning history, applications and evidence are deleted, your subscriptions are cancelled and your organisation seat is released. The record of what you bought is kept, because it is an accounting record.
- **Erasure** means forget I existed. Everything a closure deletes, and the commercial record as well, and then the account itself is removed rather than emptied.

Both are actioned in two steps that cannot be run by accident. Whoever handles it first produces a read-only preview of exactly what will be removed, including files held outside the database, and then confirms in writing. You are emailed before the account goes, and the confirmation names your member number as retired.

7.3 What survives an erasure, and why

- **The audit log**, for six years. It records what we decided about you and when, including the erasure itself. An audit log the subject can delete is not an audit log.
- **The record of your request**, for six years. It is the evidence we did what you asked, and deleting it would remove the proof that the erasure happened.
- **Your membership consent record**, for six years. It records what you agreed to and which version of the Code and the refund policy applied when you bought a membership.

- **Your member number**, permanently, as a number and a date with no name attached. It is kept so it can never be issued to somebody else, which protects the certificates and verification records that already carry it.
- **Authority to Work records**, where an employer holds them. See Section 1.2.

Nothing in this list is a way of keeping your record. Each one is either something we must be able to produce, or something that protects you after you have gone.

7.4 Where a record is about more than one person

Some records name somebody else: a reviewer who validated a level, a verifier who confirmed a claim, a colleague who gave feedback, a host who raised a concern. Those are disclosed to you with the other person's identifying detail considered separately, and a record is never withheld in full where part of it can be given.

7.5 Confirming it is you

A request from the email address on the account is treated as verified. Where it is not, we ask for enough to be confident and no more. Nobody is asked for photographic identification to obtain a copy of their own CPD log.

7.6 If you are not satisfied

Raise it under IPP-GOV-006, which is the single intake for every complaint and is answered on the timescales set out there. You may also complain to the Information Commissioner's Office at any time, before, during or after raising it with us, and you do not need our agreement to do so. ico.org.uk, helpline 0303 123 1113. Our registration reference is ZC198668.

8. Automated decisions

Award and Foundation papers are marked automatically. Each question carries one mark, there is no partial credit and no negative marking, and the pass mark is published in IPP-ASM-001. The result is produced without a human looking at it, and it decides whether you hold the qualification.

This is necessary to deliver the assessment you entered, and it is the same process applied identically to every candidate. You can ask for the decision to be looked at by a person, and IPP-ASM-001 Section 3.6 is the route: an appeal within 20 working days, decided by somebody who did not make the original decision. IPP-ASM-002 Section 9 covers what happens when one of our own questions turns out to be defective, including re-marking sittings that have already happened.

No other decision about you is made automatically. Membership admission, direct entry, reasonable adjustments, malpractice findings and Practitioner marking are all made by named people, and the two most serious of those require two of them.

9. Who processes it, and where

We use four processors. None of them may use your data for their own purposes. We sell no personal data, share nothing with advertisers or data brokers, and run no analytics or tracking service.

Processor	What it does	What it receives
Cloudflare	Hosting, the database, file storage, backups, and bot protection on public forms	Everything in Section 3, as the platform it runs on, plus your IP address and request data as part of serving a page. The bot check itself receives only a challenge token
Clerk	Identity and sign-in	Name, email address, and your membership grade, designation, member number and whether you administer an organisation
Stripe	Payments	Name, email address and what you bought. Card details go to Stripe directly and are never held by us. Stripe is not only our processor: see the note below
Resend	Sending email	Your email address, and the content of the message, which routinely includes your name and member number

Our pages fetch nothing from anybody else. Fonts, icons and code are served from our own addresses, so opening one of our pages tells nobody but us that you opened it. There is one exception, and it is the sign-in page itself: our identity provider serves its own sign-in code from its own address, which is how that provider is designed to work and which is why it is named in this section. Every other page in the estate is checked automatically and refused if it fetches from a party not named above.

Stripe has two roles and it matters which is which. When it takes a payment on our instruction it is our processor and this notice governs it. When it decides how to detect fraud, how to meet anti-money-laundering and identity obligations, which banks and processors to route through, and how to manage its own relationship with you, it is a controller in its own right, deciding those purposes itself. For that part Stripe's own privacy policy applies alongside this one and your rights are exercised against Stripe. We cannot instruct them out of obligations they carry directly.

Account and platform data is held in Cloudflare's database infrastructure within the United Kingdom and the European Economic Area. Clerk, Stripe and Resend are United States companies. Clerk and Stripe are certified under the EU-US Data Privacy Framework and use standard contractual clauses for transfers out of the UK and EEA. Resend processes only what is needed to deliver a specific email and retains it only as long as operating the service requires.

No processor is engaged without a written agreement binding it to act only on our instructions, keep the data secure, and delete or return it at the end of the engagement. Those agreements, the version of each in force, and the transfer safeguards relied on are recorded in IPP-REG-002, which is an internal control record rather than a published one. Any change to this list is made in this document at its next issue, and IPP-REG-001 records that issue.

10. Security

- Sign-in is handled by a specialist identity provider. Session tokens are stored only as a one-way hash, so a copy of the database does not let anybody sign in as you.
- Sessions expire after seven days of inactivity and after thirty days regardless. A session on a shared device expires after eight hours and does not persist.
- Access is by role, and a staff view of a subject's full record is written to the audit log.
- The database is backed up nightly, with the retention in Section 6.
- Uploaded evidence is held separately from the database and reachable only through an authorised route, never by guessing a web address.
- Public forms are protected against automated abuse.

11. Cookies, breaches and minimum age

11.1 Cookies

We use cookies only where they are strictly necessary for the platforms to work: the session cookies that keep you signed in, shared across the modulesix.io platforms so one sign-in works across them, with a separate session on ipp.pro. No advertising cookies, no analytics cookies, nothing from a third-party advertising network.

Because everything we set is strictly necessary, we are not required to ask your consent under the Privacy and Electronic Communications Regulations, and no banner is shown because there is nothing optional to consent to. Full detail at ipp.pro/cookies.

11.2 If something goes wrong

A suspected personal data breach is reported to the Governance Board without delay and assessed the same working day. Where it is likely to risk people it is reported to the Information Commissioner's Office within 72 hours of us becoming aware. Where the risk is high, the people affected are told directly, and told what to do.

Every incident is recorded whether or not it was reportable: what happened, when it was found, what data and how many people were involved, what was done, and what changed afterwards. Kept for six years.

11.3 Minimum age

Our platforms are for people aged 16 and above. Candidate membership is open to sixth form and college students preparing for professional qualifications. We do not knowingly hold personal data about anyone under 16. If you believe we do, email data@ipp.pro and it will be removed.

11.4 Changes to this document

This document is versioned rather than dated. Its current issue is recorded in IPP-REG-001, and the page at ipp.pro/privacy is generated from it, so the two change together. Where a change materially affects how we use your personal data, we tell you by email rather than relying on you noticing.

12. Related documents



Reference	What it owns that touches this document
IPP-DAT-002	The field-by-field detail of every public surface, and the labels a viewer sees
IPP-GOV-006	The single intake for a complaint, including one about privacy
IPP-GOV-005	What you may claim about your membership
IPP-GOV-007	Direct entry, and the evidence submitted with an application
IPP-GOV-008	CPD, and the fact that a CPD log is the member's own record
IPP-ASM-001	Examination format, pass marks and the assessment appeal route in Section 3.6
IPP-ASM-002	Sitting conditions, reasonable adjustments, malpractice and defective questions
IPP-REG-001	Which issue of this document is current
IPP-REG-002	The processor agreements in force and the transfer safeguards

The Institute of Project Professionals is operated by Module Six Ltd, registered in England and Wales no. 17311940, ICO reference ZC198668. IPP is not affiliated with or endorsed by APM, PMI or AXELOS.