The Institute of The Motor Industry

Organisation-wide Privacy Notice

Date policy change approved by the Board of Directors	Change occurrence	Date last reviewed	Date for next review	File stored
Aug 2026	V0.1	Initial draft		
October 2026	V0.2 added on Section 4 the word ‘may’ ‘Personal data we MAY use’			
27/10/26 SLT/EDT Approval	V1.0		2027	

Organisation-wide Privacy Notice

1. Purpose

The Institute of the Motor Industry is committed to using personal data lawfully, fairly, transparently and securely. This notice explains what personal data we use, where it comes from, why we use it, the lawful bases we rely on, who we share it with, how long we keep it and the rights available to individuals.

This notice supports the transparency requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable UK data protection and electronic communications legislation. It should be read with any shorter or more specific privacy information provided when personal data is collected.

2. Who we are and how to contact us

Item	Details
Controller	The Institute of the Motor Industry, registered in England and Wales under company number 00225180.
Registered office	Fanshaws, Brickendon, Hertford, SG13 8PQ.
ICO registration	Z5596514.
Privacy contact	GDPR@theimi.org.uk
Data Protection Officer	Evalian Limited, West Lodge, Leylands Business Park, Colden Common, Hampshire, SO21 1TH. Email: dpo@evalian.co.uk. Mark correspondence for the attention of the Data Protection Officer.

3. Who this notice applies to

This notice may apply to:

- members, prospective members and individuals listed on professional registers
- learners, candidates, apprentices, end-point assessment participants and certificate holders
- staff and representatives of IMI Approved Centres, training providers, employers and delivery partners
- customers, purchasers, delegates, speakers, volunteers, judges, entrants and event participants
- complainants, appellants, witnesses, individuals involved in malpractice, professional standards or safeguarding matters
- website, portal, application and digital-service users
- suppliers, contractors, consultants, advisers, business contacts and prospective partners
- job applicants, employees, workers, former staff, pension beneficiaries and emergency contacts
- visitors to IMI premises and people captured by security systems
- anyone contacting IMI, exercising a data protection right or whose personal data is provided to IMI by another person or organisation

4. Personal data we may use

Category	Examples
Identity and contact	Name, title, date of birth, address, email address, telephone number, identifiers, photograph and signature.
Membership and professional	Membership number, grade, status, CPD, professional registration, qualifications, employment sector, interests and disciplinary or professional standards information.
Learner, qualification and assessment	Learner or candidate number, centre, programme, registrations, assessment evidence, results, certification, reasonable adjustments, special consideration, quality assurance and malpractice information.
Employment and recruitment	CV, application, work history, qualifications, references, right-to-work evidence, contract, pay, benefits, leave, attendance, training, performance, grievance, disciplinary and pension information.
Financial and transaction	Bank details, payment information, invoices, refunds, expenses, purchase history, debt and credit-control records.
Communications and relationship	Correspondence, call notes, enquiries, complaints, appeals, survey responses, preferences, event attendance and account history.
Technical, usage and security	IP address, login records, device and browser information, audit logs, access records, website activity, security alerts and CCTV where used.
Marketing	Communication preferences, consent or objection records, campaign engagement and areas of interest.
Governance and compliance	RoPA, DPIA, LIA, DSAR, IRR rights, data breach, risk, audit, due diligence, conflict and investigation records.
Special category data	Health, disability, ethnicity, racial origin, religious or philosophical belief, trade union membership, biometric data used for unique identification, sex life or sexual orientation, where relevant and lawful.
Criminal offence data	Convictions, allegations, DBS outcomes or offence-related information, only where legally permitted and necessary.

IMI seeks to collect only personal data that is adequate, relevant and limited to what is necessary for the stated purpose. Where we ask for information that is optional, we will make this clear where practicable.

5. How we collect personal data

Directly from you: Through applications, registrations, purchases, forms, portals, assessments, emails, telephone calls, events, meetings, surveys, complaints, job applications and other interactions.

From organisations you work or study with: Including Approved Centres, training providers, employers, apprenticeship providers, assessment organisations, partners and referees.

From service providers: Including payment, identity checking, recruitment, IT, hosting, marketing, event, print, delivery and professional service providers.

From public and regulatory sources: Including Companies House, professional or public registers, regulators, law enforcement and publicly available sources where lawful.

Created during our relationship: Including membership, learner, assessment, certification, quality assurance, account, audit, correspondence, investigation, employment and governance records.

Automatically: Through websites, portals, applications, system logs, cookies and similar technologies, subject to applicable choice and consent requirements.

6. How and why we use personal data

We identify a lawful basis before processing personal data. Depending on the activity, we may rely on consent, performance of a contract, steps before entering a contract, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest where applicable, or legitimate interests.

Where legitimate interests are used, IMI considers necessity and balances its interests against the individual's rights and interests.

Appendix A: Processing activities and transparency schedule

Business area / activity	Purpose	Personal data	Lawful basis	Typical recipients	Retention approach
Membership and professional registration	Administer applications, renewals, benefits, account services, CPD, grades, registers, verification and professional standards.	Identity/contact; membership/professional; transaction; communications.	Contract; legal obligation where applicable; legitimate interests for service administration, verification and improvement.	Members, applicants, employers or public users of registers, service providers, regulatory or professional bodies where relevant.	Membership or register relationship plus applicable approved retention period.
Qualifications, learners and certification	Register learners, administer qualifications, assessments and EPA, record results, issue and replace certificates, verify achievements and maintain awarding evidence.	Identity/contact; learner/assessment; special category data for adjustments where required; communications.	Contract; legal or regulatory obligation; legitimate interests; substantial public interest or other Article 9 condition where applicable.	Approved Centres, training providers, employers, assessors, EPA partners, qualification regulators, technology and print providers.	As set out in the approved retention schedule, including longer retention where needed to verify achievements or meet regulatory conditions.
Approved Centres and quality assurance	Approve, monitor and support centres; conduct quality assurance, audits, investigations and regulatory reporting.	Business contact; centre staff; learner and assessment; audit; complaints and investigation data.	Contract; legal or regulatory obligation; legitimate interests in quality, integrity and risk management.	Centres, quality assurance personnel, regulators, auditors and relevant service providers.	Approved retention schedule and applicable regulatory requirements.

Business area / activity	Purpose	Personal data	Lawful basis	Typical recipients	Retention approach
Products, services and customer accounts	Provide purchases, subscriptions, bookings, licences, events, training and customer support; manage payments, refunds and debts.	Identity/contact; financial/transaction; profile; communications.	Contract; legal obligation; legitimate interests in administration and debt recovery.	Payment, delivery, booking, hosting and support providers; professional advisers where needed.	Contract/relationship duration plus approved financial and legal retention.
Events, awards and engagement	Manage registrations, attendance, speakers, awards, competitions, photographs, accessibility, surveys and follow-up.	Identity/contact; profile; transaction; image; health or accessibility data where necessary.	Contract; consent where appropriate; legitimate interests; legal obligation; Article 9 condition where required.	Venues, event platforms, sponsors or partners where disclosed, judges, media and service providers.	According to the approved event, marketing, finance and safeguarding retention entries.
Marketing and public affairs	Send relevant communications, manage preferences, analyse engagement, promote services and support stakeholder engagement.	Identity/contact; marketing preferences; profile; usage and communications.	Consent; legitimate interests where permitted; compliance with PECR and the right to object.	Email, CRM, analytics, advertising and communications providers.	Until opt-out, withdrawal or approved inactivity threshold, with suppression evidence retained as required.
Complaints, appeals and professional standards	Receive, investigate and resolve complaints, appeals, misconduct, malpractice and professional standards matters.	Identity/contact; communications; learner/professional; evidence; special category or criminal offence data where necessary.	Contract; legal or regulatory obligation; legitimate interests; legal claims; applicable Article 9 or Schedule 1 condition.	Relevant parties, centres, regulators, investigators, legal advisers, insurers and authorities where lawful.	Approved complaints, appeals, malpractice, legal and regulatory retention.

Business area / activity	Purpose	Personal data	Lawful basis	Typical recipients	Retention approach
Safeguarding and welfare	Receive and manage safeguarding concerns, welfare information, disclosures and referrals.	Identity/contact; health; family; allegation; special category and criminal offence data.	Legal obligation; vital interests; public interest; substantial public interest and safeguarding conditions.	Safeguarding leads, emergency services, local authorities, regulators and relevant organisations where necessary and lawful.	Approved safeguarding retention schedule, subject to legal hold and statutory guidance.
Recruitment	Assess applicants, arrange interviews, conduct checks, make offers, make adjustments and maintain recruitment records.	Identity/contact; CV; qualifications; references; interview notes; right-to-work; health or equality data where relevant.	Pre-contract steps; legal obligation; legitimate interests; consent for talent pools where appropriate; employment Article 9 condition.	Recruitment platforms, agencies, referees, screening providers and hiring managers.	Unsuccessful applicant records normally follow the approved recruitment schedule; successful records transfer to the employee file.
People and employment	Manage the employment or engagement relationship, pay, benefits, welfare, performance, training, leave, pensions, workplace safety and investigations.	Employment, financial, contact, next-of-kin, system use, health and equality data.	Contract; legal obligation; legitimate interests; vital interests; employment, social security and health Article 9 conditions.	HR, payroll, pension, benefits, occupational health, IT and professional service providers; authorities where required.	Approved HR, payroll, pension, health and safety and legal retention schedule.
Suppliers, contracts and due diligence	Onboard suppliers, perform risk and due diligence checks, manage contracts,	Business contact; identity; financial; due diligence; security and access data.	Contract; steps before contract; legal obligation; legitimate interests in	Finance, procurement, advisers, due diligence and system providers, regulators	Contract term plus approved procurement, finance and legal retention.

Business area / activity	Purpose	Personal data	Lawful basis	Typical recipients	Retention approach
	invoices, access, assurance and offboarding.		procurement, security and governance.	or authorities where required.	
Finance, tax and corporate governance	Maintain accounts, audits, statutory records, board and committee governance, insurance, fraud prevention and financial controls.	Identity/contact; transaction; governance; conflict; audit; investigation data.	Legal obligation; contract; legitimate interests; legal claims.	Banks, auditors, insurers, tax authorities, Companies House, advisers and regulators.	Approved finance, tax, governance and legal retention schedule.
IT, security and business continuity	Provide systems and accounts, monitor security, manage access, logs, incidents, backups, continuity and acceptable use.	Technical, usage, identity/contact, system content and security records.	Legal obligation; contract for staff users; legitimate interests in security, continuity and fraud prevention.	IT, cloud, security, support and incident response providers; insurers and authorities where necessary.	Approved IT, audit-log, incident and security retention schedule.
Data protection and information governance	Maintain RoPA, DPIAs, LIAs, data subject request, breach, consent, sharing, audit and compliance evidence.	Identity/contact; request and verification data; processing, risk, incident and correspondence records.	Legal obligation; legitimate interests in accountability and legal claims.	DPO, advisers, processors, insurers, regulators and authorities where required.	Approved data-protection retention schedule and any legal hold.
Premises and visitor management	Manage visitors, access, safety and security, including CCTV where used	Identity/contact; visit details; access records; images.	Legal obligation; legitimate interests in	Facilities, security, IT and law-enforcement bodies where lawful.	Approved visitor, access and CCTV retention schedule.

Business area / activity	Purpose	Personal data	Lawful basis	Typical recipients	Retention approach
	and properly signposted.		safety, security and asset protection.		
Research, insight and service improvement	Analyse feedback, trends and service use, produce statistics and improve services, preferably using anonymised or aggregated data.	Profile, usage, survey, transaction and service data.	Legitimate interests; consent where required; public task only where applicable and documented.	Research, analytics and technology providers; partners where properly governed.	Only for the validated research or improvement period, then deletion or anonymisation.

7. Special category and criminal offence data

IMI processes special category or criminal offence data only where it is necessary, proportionate and supported by both an Article 6 lawful basis and the additional legal condition required by the UK GDPR and Data Protection Act 2018. Depending on the activity, this may include employment and social security obligations, substantial public interest, safeguarding, health or social care, vital interests, legal claims, explicit consent, or data manifestly made public by the individual.

- IMI will document the relevant condition in the RoPA and, where required, an Appropriate Policy Document.
- IMI will limit access to authorised roles and share only the minimum necessary information.
- IMI will complete a DPIA where processing is likely to result in high risk.
- IMI will apply additional security, retention and deletion controls.
- IMI will avoid relying on consent where an imbalance of power means it may not be freely given.

8. Marketing and communications

IMI may send service communications that are necessary to administer a relationship, account, membership, qualification, booking or contract. These are separate from optional direct marketing.

For direct marketing, IMI will use consent where required and may use legitimate interests where the law permits. Electronic marketing will be managed in accordance with applicable privacy and electronic communications rules. Individuals can opt out at any time using the unsubscribe route in the message or by contacting IMI. IMI may retain a minimal suppression record so that the preference is respected.

IMI will not sell personal data. Any third-party or partner marketing will be clearly explained and supported by an appropriate lawful basis and marketing permission where required.

9. Cookies and digital services

IMI websites and digital services may use strictly necessary cookies and, where permission is required, optional analytics, functionality or advertising technologies. Detailed information, including purpose, provider, duration and preference controls, is set out in the separate Cookies Notice and reflected in the live consent tool.

Our website uses cookies to distinguish you from other users of our website. A cookie is a small file of letters and numbers that we put on your computer if you agree. These cookies allow us to distinguish you from other users of our website, which helps us to provide you with a good experience when you browse our website and also allows us to improve our site. The cookies we use are "analytical" cookies. They allow us to recognize and count the number of visitors and to see how visitors move around the site when they are using it. This helps us to improve the way our website works and helps us to provide you with a good experience when you browse our website and also allows us to improve our site.

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

10. Sharing personal data

IMI may share personal data with the following categories where necessary and lawful:

- IMI Approved Centres, training providers, employers, assessment bodies and delivery partners
- qualification, apprenticeship and other competent regulators
- technology, cloud, hosting, security, CRM, payment, print, logistics, event and communications providers acting as processors
- banks, auditors, insurers, pension and benefits providers, occupational health providers and professional advisers
- government departments, tax authorities, Companies House, law enforcement, courts and other public authorities
- safeguarding bodies, emergency services and relevant welfare organisations
- other controllers or joint controllers where the relationship and responsibilities are explained

Processors may act only on documented instructions, must protect personal data and must meet contractual data protection obligations. Where organisations act as separate or joint controllers, IMI will define responsibilities through an appropriate agreement or collection notice.

11. International transfers

Some suppliers or partners may store or access personal data outside the United Kingdom. Before making a restricted transfer, IMI will identify an available lawful transfer mechanism, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved Standard Contractual Clauses, or another mechanism permitted by law. IMI will complete any required transfer risk assessment and apply supplementary safeguards where appropriate.

12. Security

IMI uses proportionate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Controls may include role-based access, authentication, encryption where appropriate, logging, secure configuration, supplier assurance, backups, staff training, confidentiality requirements, incident response and secure disposal.

Access is limited to people who require it for an authorised business purpose. Suspected personal data breaches are assessed, recorded and, where legally required, reported to the ICO and affected individuals.

13. Retention

IMI keeps personal data only for as long as it is needed for the purpose for which it was collected and to meet legal, regulatory, contractual, accounting, audit and reporting requirements, or to establish, exercise or defend legal claims. Retention decisions take account of the amount, nature and sensitivity of the data, the risk of harm, the purposes of processing and whether those purposes can be achieved in another way.

Detailed periods are maintained in the approved Data Retention and Destruction Policy and Schedule.

Where a legal hold, complaint, investigation, audit or regulatory matter applies, deletion may be suspended until the hold is formally released. At the end of the retention period, data will be securely deleted, destroyed or irreversibly anonymised.

14. Automated decision-making and profiling

IMI will tell individuals if it makes a decision based solely on automated processing that produces legal or similarly significant effects. Where applicable, IMI will explain the logic involved, the significance and likely consequences, and the safeguards and rights available, including human review.

15. Your data protection rights

Depending on the circumstances, individuals may have the right to:

- be informed about the use of their personal data
- request access to their personal data
- ask for inaccurate or incomplete data to be corrected
- ask for personal data to be erased where the legal conditions apply
- ask for processing to be restricted
- object to processing based on legitimate interests and object at any time to direct marketing
- receive certain personal data in a portable format and have it transmitted to another controller where applicable
- withdraw consent at any time where consent is the basis for processing
- not be subject to a solely automated decision with legal or similarly significant effects, subject to legal exceptions and safeguards
- complain to the Information Commissioner's Office

Rights are not absolute and may be limited by law. IMI may ask for information needed to confirm identity and clarify the request. Requests are normally free of charge, although the law permits a reasonable fee or refusal in limited circumstances involving manifestly unfounded or excessive requests. IMI will respond within the statutory timescale and explain any permitted extension or refusal.

To exercise a right, contact GDPR@theimi.org.uk or the Data Protection Officer, Evalian dpo@evalian.co.uk

16. Children and young people

Some IMI services may involve children or young people, including through qualifications, training, competitions, events, digital services or safeguarding activities. Where this occurs, IMI will provide privacy information in clear and age-appropriate language, apply data minimisation and suitable access controls, identify the correct lawful basis and additional condition, and consider whether a DPIA is required.

Where consent is relied on for an online service offered directly to a child, IMI will apply the applicable UK age and parental authorisation requirements. IMI will not assume that parental consent is the lawful basis for all processing involving a child.

17. Complaints

If you are concerned about how IMI uses your personal data, please contact IMI or the Data Protection Officer first so that the matter can be investigated. You may also complain to the Information Commissioner's Office (ICO), the UK supervisory authority. Current contact routes are available at https://ico.org.uk/make-a-complaint.

18. Changes to this notice

IMI keeps this notice under review and will update it when processing activities, systems, suppliers, laws or regulatory expectations change. Material changes will be communicated through appropriate channels. The published notice will show its effective date and version.

19. Related documents

- Information Governance and Data Protection Policy
- Data Retention and Destruction Policy and Schedule
- Employee, Worker, Consultant and Contractor Privacy Notice
- Job Applicant Privacy Notice
- Website Privacy Notice and Cookies Notice
- Data Subject Rights Procedure
- Appropriate Policy
- DPIA Procedure and Template
- Legitimate Interests Assessment Procedure and Template
- Personal Data Breach Procedure
- Data Sharing and Data Processing Agreement templates
- Information Security and Cyber Incident Response documentation
- RoPA and governance registers

Appendix B: Publication and validation checklist

Check	Required action
Corporate details	Confirm controller name, company number, address and ICO registration.
Ownership and approval	Confirm owner, approver, effective date, next review date and document reference.
DPO and privacy contacts	Insert tested contact routes and confirm DPO wording.
RoPA alignment	Validate every row in Appendix A against current processing activities and departmental owners.
Lawful basis	Confirm Article 6 basis for every purpose and legitimate interest wording against LIAs.
Special category / offence data	Confirm Article 9 and DPA 2018 Schedule 1 conditions and Appropriate Policy Document requirements.
Recipients	Replace generic categories with accurate, meaningful categories and identify named recipients where necessary for transparency.
International transfers	Confirm countries, transfer mechanism, transfer risk assessments and supplementary measures.
Retention	Cross-check every summary against the approved retention schedule; remove unapproved periods.
Automated decisions and AI	Verify whether legally or similarly significant solely automated decisions occur and add activity-specific wording.
Children	Identify services used by children and test the notice for age-appropriate transparency.
Cookies and PECR	Complete cookie audit, validate consent functionality and publish a separate Cookies Notice.
Collection points	Add layered links to forms, portals, membership journeys, centres, event bookings, recruitment and staff systems.
Accessibility	Test headings, links, reading order, contrast, mobile display and plain-English readability.
Contracts and suppliers	Confirm controller/processor roles and Article 28 terms for relevant suppliers.
Regulatory review	Validate awarding and qualification content with relevant operational and regulatory owners.
DPO review	Obtain documented DPO advice and record whether recommendations were accepted.

Check	Required action
Superseded content	Archive prior versions and update all links, templates, training and internal references.
Governance evidence	Record approval, publication, communications and annual review in the Policy Register.