DATA PROTECTION POLICY

Issue Number	Effective Date	Amendments	Reason for Amendments

INTRODUCTION

The Institute of the Motor Industry (IMI) needs to gather and use certain information about individuals.

These can include learners, members, customers, business contacts, suppliers, employees and other people the organisation has a relationship with and may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organisation's data protection standards and to comply with the law.

WHY THIS POLICY EXISTS

This data protection policy ensures the IMI:

- Complies with the data protection law and follows good practice
- Protects the rights of employees, customers and partners
- Is transparent in how it processes and stores individuals' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW

The Data Protection Act (1998) describes how organisations – including the IMI – must collect, handle and store personal information.

These rules apply regardless of whether the data is stored electronically, on paper or on other media.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up-to-date
- Not be held for longer than is necessary
- Processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

From 25th May, 2018 new EU data protection legislation will come into effect, called The General Data Protection Regulation (GDPR). This legislation enhances the Data Protection Act in two important areas:

Individuals data rights are enhanced (see section on Subject Access Requests) and the types of information classified as personal information has been expanded.

Organisations like the IMI have additional responsibilities around demonstrating accountability and governance in how we process personal data and also in how we log and report data breaches (see Data Breach Notification Policy).

PEOPLE, RISK AND RESPONSIBILITIES

POLICY SCOPE

This policy applies to:

- The Head Office (Fanshaws) of the IMI
- All remote sites (including homeworkers) of the IMI
- All staff and volunteers of the IMI
- All contractors, suppliers and other people working on behalf of the IMI

It applies to all information the organisation holds about identifiable individuals, even if that information technically falls outside of the Data Protection Act/GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Candidate numbers
- Membership details
- Payment details
- Plus any other information relating to individuals

This policy does not apply to information the organisation holds on employees. The protection of personal information on employees is covered within the HR Policies Staff Handbook under the section entitled 'Confidentiality and Data Protection Policy'.

DATA PROTECTION RISKS

This policy helps to protect the IMI from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

RESPONSIBILITIES

Everyone who works for or with the IMI has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these groups & people have key areas of responsibility:

- The Executive Director Team (EDT) & Board is ultimately responsible for ensuring that the IMI meets its legal obligations.

- The Senior Management Team (SMT), is responsible for:
  - Keeping the EDT & Board updated about data protection responsibilities, risks and issues
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule
  - Arranging data protection inductions, training and advice for the people covered by this policy
  - Handling data protection requests from staff and anyone else covered by this policy
  - Dealing with requests from individuals to see the data the IMI holds about them (also called Subject Access Requests)
  - Checking and approving any contracts or agreements with third parties that may handle the organisation's sensitive data
  - Decision on whether to notify ICO regarding a data breaches

- The Head of IT is responsible for:
  - Ensuring all systems, services and equipment used for storing data meets acceptable security standards
  - Performing regular checks and scans to ensure security hardware and software is functioning properly
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services

- The Head of Marketing & Communications is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters
  - Addressing any data protection queries from journalists or media outlets like newspapers
  - Working with other members of SMT to ensure marketing initiatives abide by data protection principles

- The Head of External Quality & Assessment Services is responsible for:
  - Managing data protection obligations for regulatory compliance purposes
  - Working with other members of SMT to ensure the IMI remains compliant in matters of data protection from a regulatory perspective

- All Staff are responsible for:
  - Following the policies and procedures approved by the IMI

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- The IMI will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared. Passwords will be changed at a maximum of every 60 days.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or a member of SMT if they are unsure about any aspect of data protection.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to your line manager or the Head of IT.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

This policy also applies to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed at least every 60 days and never shared between employees.
- Removable media (like a CD, DVD or tape) should and Memory sticks should never be used to store personal data as covered by this policy.
- Data should only be stored on designated drives and servers, and should only be uploaded to the approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. These backups should be tested regularly, in line with the company's standard backup procedures.
- Personal Data should never be saved directly to laptops of other mobile devices like tablets or smartphones.

All servers and computers containing data should be protected by approved security software and a firewall

DATA USE

Personal data is of no value to the IMI unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email or as an email attachment, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The Head of IT can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

DATA ACCURACY

The law requires the IMI to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is the personal data is accurate, the greater the effort the IMI should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- The IMI will make it easy for data subjects to update the information we hold about them. For instance, via client portals on the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

SUBJECT ACCESS REQUESTS

Under GDPR, individuals who are the subject of personal data held by the IMI are entitled to:

- The right to be informed with clear, transparent and easily understandable information about how we use their personal data.
- The right to obtain their personal data.
- The right to request that the IMI corrects any personal data found to be inaccurate or out of date.
- The right to request that their personal data is erased where it is no longer necessary for the IMI to retain such data.
- The right to restrict processing of their personal data in certain circumstances.
- The right to obtain and reuse their personal data in a structured, commonly used and readable format, known as the right to "data portability."
- The right to object to us processing their personal data for our legitimate business interests or for direct marketing purposes.
- The right to withdraw their consent to processing.
- The right to lodge a complaint with the Information Commissioners Office.

If an individual contacts the IMI with an above request, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Controller at dataquestions@theimi.org.uk. A standard request form is enclosed in Appendix (2), although individuals do not have to use this.

The IMI will aim to provide the relevant data within 1 calendar month from receipt of the request.

It is our obligation to always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the IMI will disclose the requested data. However, the IMI will ensure the request is legitimate and accompanied by a court order, seeking assistance from the board and from the organisation's legal advisors where necessary.

PROVIDING INFORMATION

The IMI aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the IMI has a privacy statement, setting out how data relating to individuals is used by the organisation.

This is available on request. A version of this statement is also available on our website.

APPENDIX 1 - SYSTEM AND DATA OWNERS

System	QLMS
Description	Database containing personal data of all candidates undertaking both regulated & unregulated IMI qualifications & accreditations. System is accessed by both the IMI and IMI approved centre network (business partners). Access to core system is
Data type	Personal data - Candidate registration/claim details.
Business Owner	Head of Membership & Professional Registration
Data Owner	Head of Membership & Professional Registration
Data Steward	IT (Amco/Aptech) External Quality & Assessment Services
Data Producer	IMI Qualification & Accreditation information. IMI Approved centre network for registration and claim information.
Data Consumer	IMI Approved Centres
Additional Notes	Centres use Web Portal 2 for both candidate registrations and claims. Access to the core application is restricted to approved IMI users only. System also has an accreditation portal for managing specific system requirements relating to accreditations. Interfaces to LMS, Accreditation Portal (separate database), ePortfolio & ProDrive. APIs from Centres Hub.

System	LMS
Description	Database managing online tests for candidates registered via QLMS
Data type	Personal data – Candidate online tests
Business Owner	Head of Product Development
Data Owner	Head of Membership & Professional Registration
Data Steward	IT (Amco/Aptech) External Quality & Assessment Services
Data Producer	Product Development
Data Consumer	IMI Approved Centres and Registered Candidates
Additional Notes	System is linked to QLMS. If a learner is eligible for an online test for their qualification then it will appear in LMS. Access to the system is managed via IMI Approved Centres.

System	Perception
Description	Database containing IMI online test question bank
Data type	MSQL RDBMS
Business Owner	Head of Product Development
Data Owner	Head of Product Development
Data Steward	IT (Amco for hosting / Questionmark for system)
Data Producer	Product Development
Data Consumer	IMI Approved Centres Registered Candidates
Additional Notes	This is a hosted application. IMI licence is for up to 75000 candidates per year.

System	360 System
Description	Multiple instanced databases containing behavioural test data for IMI staff and customers
Data type	MSQL RDBMS
Business Owner	Head of External Quality & Assessment Services
Data Owner	Head of External Quality & Assessment Services – Approved Centre Data Head of Membership & Professional Registration – Individual Data Head of HR & Business Support – IMI Employee Data
Data Steward	IT (Amco/Aptech) External Quality & Assessment Services
Data Producer	IMI Approved Centres IMI
Data Consumer	IMI Approved Centres IMI
Additional Notes	System is compartmentalised into separate databases to ensure data security in maintained.

System	ePortfolio
Description	Electronic log book used by candidates undertaking IMI qualifications.
Data type	Personal data – evidence based learner outcomes.
Business Owner	Head of External Quality & Assessment Services
Data Owner	Head of Membership & Professional Registration – Individual data Head of External Quality & Assessment Services – Approved Centre data
Data Steward	IT (Amco/Aptech) External Quality & Assessment Services
Data Producer	Registered candidates IMI Approved Centres
Data Consumer	Registered candidates IMI Approved Centres
Additional Notes	Backup currently consuming around 44TB of data. This is a hosted application and linked to QLMS.

System	Centres Hub
Description	Centre Management system
Data type	Approved Centre data Qualification data External Quality & Assessment Services data
Business Owner	Head of External Quality & Assessment Services
Data Owner	Head of External Quality & Assessment Services
Data Steward	IT (Creatio) External Quality & Assessment Services
Data Producer	External Quality & Assessment Services IMI Approved Centres
Data Consumer	External Quality & Assessment Services IMI Approved Centres
Additional Notes	Currently linked to QLMS via basic APIs. Generates centre PIN for access to systems.

System	Digital Certificates
Description	Certification platform for candidates
Data type	Personal data
Business Owner	Head of Membership & Professional Registration
Data Owner	Head of Membership & Professional Registration
Data Steward	IT (Amco/Advanced Secure)
Data Producer	Candidate data
Data Consumer	IMI Approved Centres Candidates
Additional Notes	Includes eModule. Linked to QLMS. Currently being scoped to add Membership certification.

System	NVQ System
Description	Legacy system
Data type	Candidate data
Business Owner	Head of Membership & Professional Registration
Data Owner	Head of Membership & Professional Registration
Data Steward	IT (Amco/Aptech)
Data Producer	None - legacy
Data Consumer	Historical candidate data
Additional Notes	System will eventually be phased out.

System	ProDrive
Description	Central data repository for data in the IMI. Data master system
Data type	Personal Data – Membership/CPD/Payment/User account data Business Data Approved Centre Data Qualification Data
Business Owner	Head of IT
Data Owner	Head of Membership & Professional Registration - individual Head of Business Development & Sales - organisation Head of External Quality & Assessment Services – IMI approved centre Product Development - Qualifications
Data Steward	IT (Camart/Achorda)
Data Producer	Individuals interacting with IMI online M & PR
Data Consumer	Individuals interacting with IMI online M & PR
Additional Notes	Modular system: Membership Module CPD Module Contacts Module Payments Gateway Module TIOG Module Quals Module Professional Register

System	Legacy Membership Database (MS Access)
Description	Legacy data for Membership
Data type	Personal data
Business Owner	Head of Membership & Professional Registration
Data Owner	Head of Membership & Professional Registration
Data Steward	IT (Amco/Aptech)
Data Producer	Membership & Professional Registration
Data Consumer	Membership & Professional Registration
Additional Notes	Currently read-only and will eventually be decommissioned (tbc).

System	Simply HR
Description	HR software for managing contractual information & employee absences.
Data type	Personal data (employee)
Business Owner	Head of HR & Business Support
Data Owner	Head of HR & Business Support
Data Steward	IT (Amco)
Data Producer	HR & Business Support Employees
Data Consumer	HR & Business Support Employees
Additional Notes	None

System	Sage Payroll
Description	Software used jointly by HR & Finance to manage IMI payroll.
Data type	Personal data (employee)
Business Owner	Head of HR & Business Support
Data Owner	Head of HR & Business Support
Data Steward	IT (Amco)
Data Producer	HR & Business Support Finance
Data Consumer	HR & Business Support Finance SMT/EDT
Additional Notes	None

System	Sage 200
Description	Accounting software used by Finance to manage debtors & creditors.
Data type	Business data (financial)
Business Owner	Head of Finance
Data Owner	Finance SMT/EDT
Data Steward	IT (new contract with Sage accredited company)
Data Producer	Finance SMT/EDT
Data Consumer	Finance SMT/EDT
Additional Notes	None

System	Desk Alerts
Description	Communications tool
Data type	Business (internal comms)
Business Owner	Head of IT
Data Owner	Various (see below)
Data Steward	IT (Amco)
Data Producer	HR & Business Support Marcomms IT Social committee
Data Consumer	All staff
Additional Notes	Will not be renewed.

System	Tableau
Description	Business intelligence and analytics software
Data type	Personal data Business data IMI Approved Centre data Financial data
Business Owner	Head of Research & ROI
Data Owner	Head of Membership & Professional Registration (personal) Head of Business Development & Sales (business) Head of External Quality & Assessment Services (Approved Centre) Head of Finance (financial)
Data Steward	IT with ROI and Research
Data Producer	ROI and Research
Data Consumer	ROI and Research SMT/EDT
Additional Notes	Limited by licence. We have issues with payments which need paying on credit card.

System	Stata
Description	Statistics and data analysis software
Data type	Personal data Business data IMI Approved Centre data Financial data
Business Owner	Head of Research & ROI
Data Owner	Head of Membership & Professional Registration (personal) Head of Business Development & Sales (business) Head of External Quality & Assessment Services (Approved Centre) Head of Finance (financial)
Data Steward	ROI and Research
Data Producer	ROI and Research
Data Consumer	ROI and Research SMT/EDT
Additional Notes	None

System	Pure360/Adestra
Description	Mass email solution
Data type	Personal data
Business Owner	Head of Marcomms
Data Owner	Head of Membership & Professional Registration
Data Steward	Marcomms IT
Data Producer	Marcomms
Data Consumer	External recipients Marcomms Membership & PR
Additional Notes	Transitioning from Pure360 to Adestra.

System	MS Exchange
Description	Mail database used for unsecured email correspondence.
Data type	Emails & attachments
Business Owner	Head of IT
Data Owner	Individual mailboxes are the responsibility of the named user.
Data Steward	IT (Amco)
Data Producer	All staff
Data Consumer	Employees & external parties
Additional Notes	Retention details applies to all emails stored in mail server.

System	Websites
Description	IMI website family: • TIOG (Corporate site) • Awarding • Autocity • Intranet
Data type	Personal data Business data IMI Approved Centre data Financial data
Business Owner	Head of Marcomms
Data Owner	Head of Membership & Professional Registration (personal) Head of Business Development & Sales (business) Head of External Quality & Assessment Services (Approved Centre) Head of Finance (financial)
Data Steward	Marcomms (front end) IT (back end and platform)
Data Producer	Customers Content Editors (various)
Data Consumer	All customers
Additional Notes	TIOG Includes: • Careers Platform • IMI Digital Magazine • Student Membership • Client Portals

	Will be transitioning to a single site model during 2017/18

System	**Moodle LMS**
Description	e-learning platform
Data type	Personal data Business data IMI Approved centre data
Business Owner	Head of Product Development
Data Owner	Head of Membership & Professional Registration (personal) Head of Business Development & Sales (business) Head of External Quality & Assessment Services (Approved Centre) Head of Product Development (product)
Data Steward	IT (Camart/AWS)
Data Producer	Product Development
Data Consumer	Customers
Additional Notes	Moved to elastic cloud platform Jan 17

System	**MS Dynamics CRM**
Description	Legacy CRM system
Data type	Business
Business Owner	None – to be removed
Data Owner	Head of Business Development & Sales (until system is decommissioned)
Data Steward	IT (Amco)
Data Producer	None
Data Consumer	None
Additional Notes	Will be decommissioned asap

System	**IMI Fileshares (folders)**
Description	Data storage for business and personal information
Data type	Personal data Business data IMI Approved Centre data Financial data
Business Owner	Head of IT
Data Owner	Head of Membership & Professional Registration (personal) Head of Business Development & Sales (business) Head of External Quality & Assessment Services (Approved Centre) Head of Finance (financial)
Data Steward	IT (Amco)
Data Producer	Employees
Data Consumer	Employees
Additional Notes	Data cleansing activities to be reviewed

System	Invu Series 6
Description	Electronic document storage/archiving solution
Data type	Personal data Business data IMI Approved Centre data Financial data
Business Owner	Head of IT
Data Owner	Head of Membership & Professional Registration (personal) Head of Business Development & Sales (business) Head of External Quality & Assessment Services Approved Centre) Head of Finance (financial)
Data Steward	IT (Amco)
Data Producer	Employees
Data Consumer	Employees
Additional Notes	Data cleansing activities to be reviewed

System	Pipedrive
Description	Cloud based Sales Pipeline system
Data type	Business
Business Owner	Head of Business Development & Sales
Data Owner	Head of Business Development & Sales
Data Steward	IT
Data Producer	Business Development & Sales
Data Consumer	Business Development & Sales Membership & Professional Registration External Quality & Assessment Services
Additional Notes	New system deployed March 2017

APPENDIX 2 – SUBJECT ACCESS REQUEST FORM

Data Controller – Subject Access
The Institute of the Motor Industry
Fanshaws
Brickendon
Herts
SG13 8PQ

Subject Access Request

Internal Use Only

SAR ID

Completed/declined date

Your Personal Details:

Mr | | Mrs | | Miss | | Ms |

Full Name:

Address:

Post Code:
Email Address:

Your Request Details:

Membership Number:

Candidate Number:

Date From: Date To:

Financial information:

Other information: e.g. CPD information, account notes, correspondence, certification information (please be as specific as possible)

How would you prefer your information? (Please select one option):

By post: | | By email |

Declaration (**must be signed**):

Please send me a copy of the requested personal data the IMI hold on file about me. I am the same person as detailed above that I am asking about.

Signed: Date: