



DATA BREACH NOTIFICATION POLICY

Issue Number	Effective Date	Amendments	Reason for Amendments
4	15/05/2024	<ol style="list-style-type: none">Amended the list of technological measures for detecting incidents in paragraph 3.1.Amended the job title of the appointed person in paragraphs 2.1 and 10.1.Amended 5.3, 6.3 and 6.4 to include OneTrust link in replacement of manual forms being emailed.Amended 7.4 and added Schedule 1.	<ol style="list-style-type: none">Changes to technological measures for data breach management.Change of responsibility within SMT.Change of process/addition of OneTrust system.Created template for notifying subjects of data breaches.

1. INTRODUCTION

- 1.1 This policy sets out the policies and procedures of The Institute of the Motor Industry (the "company") with respect to detection of personal data breaches, responding to personal data breaches and notification of personal data breaches to supervisory authorities, data controllers and data subjects.
- 1.2 When dealing with personal data breaches, the company and all company personnel must focus on protecting individuals and their personal data, as well as protecting the interests of the company.

2. DEFINITIONS

- 2.1 In this policy:
 - a) "**appointed person**" means the individuals primarily responsible for dealing with personal data breaches affecting the company, being a member of the Senior Management Team or another IMI manager appointed by the Senior Management Team;
 - b) "**data controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
 - c) "**data processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
 - d) "**data subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
 - e) "**personal data**" means any information relating to a data subject;
 - f) "**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the company (including any temporary or permanent loss of control of, or inability to access, personal data); and
 - g) "**supervisory authority**" means the Information Commissioner's Office of the United Kingdom.

3. DETECTION OF PERSONAL DATA BREACHES

- 3.1 The company has put in place technological measures to detect incidents which may result in personal data breaches. As at the date of this policy, those measures include:
 - a) a data governance audit & compliance tool (Varonis migrating to Microsoft 365 DLP);

- b) an anti-virus/malware tool (Microsoft 365 Defender);
- c) an anti-spam/phishing tool (Fusemail);
- d) a firewall (Dell Sonicwall); and
- e) a centralised CRM (ProDrive and Centres Hub).

3.2 The company has put in place organisational measures to detect incidents which may result in personal data breaches. As at the date of this policy, those measures include:

- a) staff awareness and training;
- b) an anti-phishing e-learning course;
- c) Data Protection Policies and Procedures;
- d) Compliance audits of our centre network.

3.3 The company shall regularly review the technical and organisational measures it uses to detect incidents which may result in a personal data breach. Such reviews shall be carried out at least annually.

4. RESPONDING TO PERSONAL DATA BREACHES

4.1 All staff of the company must notify the appointed person immediately if they become aware of any actual or possible personal data breach. The appointed person must record the breach in the data breach register so the breach can be time stamped and if necessary a ticket should be logged with IT support if the breach is a systems issue.

4.2 The appointed person is primarily responsible for investigating possible and actual personal data breaches and for determining whether any notification obligations apply. Where notification obligations apply, the appointed person is responsible for ensuring notification of the relevant third parties in accordance with this policy.

4.3 All personnel of the company must cooperate with the appointed person in relation to the investigation and notification of personal data breaches.

4.4 The appointed person must determine whether the company is acting as a data controller and/or a data processor with respect to each category of personal data that is subject to a personal data breach. The company is likely to act as a data controller in relation to the following categories of personal data:

- a) IMI Membership (including Student Membership);
- b) IMI Accreditation;
- c) Regulated Qualifications;
- d) eLearning (including MOT)

e) Online user accounts (IMI websites)

The company is likely to act as a data processor in relation to the following categories of personal data:

f) IRTEC

g) some QAPs

The company's status as controller or processor must be checked and verified by the appointed person in every instance.

4.5 The steps to be taken by the appointed person when responding to a personal data breach may include:

a) ensuring that the personal data breach is contained as soon as possible;

b) assessing the level of risk to data subjects as soon as possible;

c) gathering and collating information from all relevant sources;

d) considering relevant data protection impact assessments;

e) informing all interested persons within the company of the personal data breach and the investigation, including relevant;

f) assessing the level of risk to the company; and

g) notifying supervisory authorities, data controllers, data subjects and others of the breach in accordance with this policy.

4.6 The appointed person shall keep a full record of the response of the company to a personal data breach, including the facts relating to the personal data breach, its effects and the remedial action taken. This record shall form part of the personal data breach register of the company.

5. NOTIFICATION TO SUPERVISORY AUTHORITY

5.1 This section 5 applies to personal data breaches affecting personal data with respect to which the company is acting as a data controller.

5.2 The company must notify the supervisory authority of any personal data breach to which this section 5 applies without undue delay and, where feasible, not later than 72 hours after the company becomes aware of the breach, save as set out in subsection 5.4.

5.3 Personal data breach notifications to the supervisory authority must be made by the appointed person using [Privacy Web Form \(onetrust.com\)](https://www.onetrust.com/privacy-web-form). The appointed person must keep a record of all notifications, and all other communications with the supervisory authority relating to the breach, as part of the personal data breach register of the company.

- 5.4 The company will not notify the supervisory authority of a personal data breach where it is unlikely to result in a risk to the rights and freedoms of natural persons. The appointed person shall be responsible for determining whether this subsection 5.4 applies, and the appointed person must create a record of any decision not to notify the supervisory authority. This record should include the appointed person's reasons for believing that the breach is unlikely to result in a risk to the rights and freedoms of natural person. This record shall be stored as part of the personal data breach register of the company.
- 5.5 To the extent that the company is not able to provide to the supervisory authority all the information required in [Privacy Web Form \(onetrust.com\)](#) at the time of the initial notification to the supervisory authority, the company must make all reasonable efforts to ascertain the missing information. That information must be provided to the supervisory authority, by the appointed person, as and when it becomes available. The appointed person must create a record of the reasons for any delayed notification under this subsection 5.5. This record shall be stored as part of the personal data breach register of the company.
- 5.6 The company must keep the supervisory authority informed of changes in the facts ascertained by the company which affect any notification made under this section 5.

6. NOTIFICATION TO DATA CONTROLLER

- 6.1 This section 6 applies to personal data breaches affecting personal data with respect to which the company is acting as a data processor.
- 6.2 The company must notify the affected data controller(s) of any personal data breach to which this section 6 applies without undue delay and, where feasible, not later than 24 hours after the company becomes aware of the breach. In addition, the company must comply with the provisions of the contract(s) with the affected data controller(s) relating to such notifications.
- 6.3 Personal data breach notifications to the affected data controller(s) must be made by the appointed person using the form [Privacy Web Form \(onetrust.com\)](#). The appointed person must keep a record of all notifications, and all other communications with the affected data controller(s) relating to the breach, as part of the personal data breach register of the company.
- 6.4 To the extent that the company is not able to provide to the affected data controller(s) all the information specified in [Privacy Web Form \(onetrust.com\)](#) the time of the initial notification to the affected data controller(s), the company must make all reasonable efforts to ascertain the missing information. That information must be provided to the affected data controller(s), by the appointed person, as and when it becomes available.

7. NOTIFICATION TO DATA SUBJECTS

- 7.1 This section 7 applies to personal data breaches affecting personal data with respect to which the company is acting as a data controller.
- 7.2 Notifications to data subject under this section 7 should, where appropriate, be made in consultation with the supervisory authority and in accordance with any guidance given by the supervisory authority with respect to such notifications.

- 7.3 The company must notify the affected data subjects of any personal data breach to which this section 7 applies if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, save as set out in subsection 7.5.
- 7.4 Personal data breach notifications to the affected data subjects must be made by the appointed person in clear and plain language using the template set out in schedule 1 (Notification of personal data breach to data subject). The completed letter must be sent to the affected data subjects by encrypted email. The appointed person must keep a record of all notifications, and all other communications with the affected data subjects relating to the breach, as part of the personal data breach register of the company.
- 7.5 The company has no obligation to notify the affected data subject of a personal data breach if:
- a) the company has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption), and those measures have been applied to the personal data affected by the personal data breach;
 - b) the company has taken subsequent measures which ensure that a high risk to the rights and freedoms of data subjects is no longer likely to materialise;
 - c) it would involve disproportionate effort (in which case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner),

Providing that the appointed person shall be responsible for determining whether this subsection 7.5 applies, and the appointed person must create a record of any decision not to notify the affected data subjects. This record should include the appointed person's reasons for believing that the breach does not need to be notified to the affected data subjects. This record shall be stored as part of the personal data breach register of the company.

- 7.6 If the company is not required by this section 7 to notify affected data subjects of a personal data breach, the company may nonetheless do so where such notification is in the interests of the company and/or the affected data subjects.

8. OTHER NOTIFICATIONS

- 8.1 Without affecting the notification obligations set out elsewhere in this policy, the appointed person should also consider whether to notify any other third parties of a personal data breach. Notifications may be required under law or contract. Relevant third parties may include:
- a) the police;
 - b) other law enforcement agencies;
 - c) insurance companies;
 - d) professional bodies;
 - e) regulatory authorities;

- f) financial institutions; and/or
- g) trade unions or other employee representatives.

9. THIRD PARTY DATA BREACH

- 9.1 If unprotected personal data is received by the IMI from a third party, IMI staff should advise the sender that it could be considered a data breach and that the personal data will be deleted by the IMI.

10. REVIEWING AND UPDATING THIS POLICY

- 10.1 An IMI manager/member of staff nominated by the Senior Management Team shall be responsible for reviewing and updating this policy.
- 10.2 This policy must be reviewed and, if appropriate, updated annually on or around March/April.
- 10.3 This policy must also be reviewed and updated on an ad hoc basis if reasonably necessary to ensure:
- a) the compliance of the company with applicable law, codes of conduct or industry best practice;
 - b) the security of data stored and processed by the company; or
 - c) the protection of the reputation of the company.
- 10.4 The following matters must be considered as part of each review of this policy:
- a) changes to the legal and regulatory environment;
 - b) changes to any codes of conduct to which the company subscribes;
 - c) developments in industry best practice;
 - d) any new data collected by the company;
 - e) any new data processing activities undertaken by the company; and
 - f) any security incidents affecting the company.



SCHEDULE 1 - Notification of personal data breach to data subject

Date of Notice

Name of the data subject

Address of the data subject

Dear **NAME**

NOTICE OF DATA BREACH

We value all our customers and respect their data privacy. However, we are writing to inform you about a data security incident involving your information. We are giving you this notice as a potentially affected individual and recommend some actions to help you protect yourself from identity theft or other fraud.

Data Breach Incident

Describe the incident briefly with the date of the incident and how long the incident continued.

Mention the date on which the incident was discovered. If the notice was delayed, then provide a reason for the same.

Personal Information Involved

The data breach incident might have involved the following personally identifiable information:

- *Name*
- *Address*
- *Birthdate*
- *Phone number*

However, the following information was not accessed:

- *Credit card number*
- *Bank account number*

Actions We've Taken



As ardent supporters of data privacy, we deeply regret this data breach incident. We assure you that we are doing our best to investigate the incident thoroughly. We have employed a well-known cyber security firm *(name of the firm)* to help us with the task. They will also set up additional security to prevent such incidences in the future.

We have also informed the law enforcement departments and have promised our full cooperation in their investigation.

What Steps You Should Take

To protect yourself from any potential resulting fraud or identity theft issues, we recommend you follow some actions:

List precise actions to be followed by the data subject.

Important Contact Information

For further information or any questions on the incident, you can contact us:

Name of the company representative

Contact information of the company representative

You can also visit [Information Commissioner's Office \(ICO\) website](#).

Yours sincerely

Chief Operating Officer