IAM Data Protection Policy

Also known as the Privacy Notice

Statement of purpose

This policy sets out how we will look after your (data subject's) information. This includes what you tell us about yourself, what we learn about you, and the choices you give us about what marketing you want us to send to you. It also provides details of your privacy rights and how to exercise those rights with us.

We are committed to promote privacy and compliance by implementing a 'Privacy by Design' approach in our business activities.

The policy can be found at http://instam.org/pdf/privacy/data-protection-policy.pdf

Policy Owner

Data Protection Officer (dataprotection@instam.org)

Related Policies, Procedures and Work Instructions

- Data Rights Form
- Data Retention Policy
- IAM Safeguarding of the Child and Vulnerable Adults Policy (IQG/0.1/007a)

Regulatory References

A, B, C, G, H, I

Scope

This policy applies to all data processed by the IAM, and affects anyone that may be considered a data subject that is processed by the IAM. This includes employees, members, attendees at IAM events, subcontractors and partners.

Who we are

The Institute of Administrative Management (Company number: **09016031)** is registered with the Information Commissioner's Office (ICO) - Registration number **ZA314023** (first registration 5 February 2018)**.**

We are part of a group of associated UK-based organisations which includes IQ Verify and the Industry Qualifications (IQ) awarding body. Data for each organisation is maintained separately. We will only transfer your data to a group organisation where we have a legal basis for doing so.

How we treat your information

We aim to ensure that all personal data is:

- processed fairly and lawfully
- obtained and processed only for specified and lawful purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- held securely and for no longer than is necessary.

We will process your data when we have a legal basis for processing it. In doing so, we will take appropriate technical and organisational measures to prevent your data from inappropriate disclosure. When a data breach occurs, we will take steps to inform you without unnecessary delay.

In processing your information we may provide it to relevant third parties such as our suppliers and enforcement agencies where we have a legal basis for doing so. We will never sell your personal information.

Where do we get your personal data and what personal data do we collect?

We may collect and process the following personal data:

Information which you freely provide to us

For example when you:

- complete a survey or form,
- correspond with us by phone, e-mail, or in writing,
- sign up to receive notifications / messages from us,
- apply to work for us,
- enter into a contract with us to receive products and/or services.

We may need to collect personal information by law, or to enter into or fulfil a contract we have with you.

If you choose not to give us this personal information, it may delay or prevent us from fulfilling our contract with you, or doing what we must do by law. It may also mean that we cannot run your accounts or policies. It could mean that we cancel a product or service you have with us.

We sometimes ask for information that is useful, but not required by law or a contract. We will make this clear when we ask for it. You do not have to give us these extra details and it won't affect the products or services you have with us.

Information we collect about you on our website

If you visit our websites, we may automatically collect the following information:

- technical information, including the internet protocol (IP) address used to connect your computer to the Internet, login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;
- information about your visit to our Website such as the products and/or services you searched for and viewed, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.

We do this by using cookies, a small file that is sent by our web server to your computer, which we can access when you make return visits to our website. For more information please see our website privacy policy: http://instam.org/data-protection-policy

Information we receive from other sources / third parties

As part of our role, we may collect and process personal data that is provided to us by our customers without direct access to data subjects.

By providing personal information to us, you give consent to IAM for processing the data as set out within this document, and you confirm that you have obtained the appropriate consent from the relevant individuals for the personal data to be processed accordingly by IAM. We reserve our right to refuse to process information received from you if we have reasonable suspicion that data subjects have not provided consent, or where we feel that there is no legitimate basis for processing.

Information about other people

If you provide information to us about any person other than yourself, such as your relatives, next of kin, your advisers or your suppliers, you must ensure that they understand how their information will be used, and that they have given their permission for you to disclose it to us and for you to allow us, and our outsourced service providers, to use it.

We may refuse to process information about other people if we have reasonable suspicion that they have not provided their consent, or where we feel that there is no legitimate basis for processing.

Sensitive personal data

Sensitive personal information includes information about your:

- racial or ethnic origin,
- political opinions,
- religious or similar beliefs,
- trade union activities,
- physical or mental health condition ,
- sexual orientation

- details of any commission or alleged commission of offences
- genetic or biometric data

In certain cases, we may need to process sensitive personal data from you. We aim to minimise collecting this information so far as possible, and will only collect and process this information if it is absolutely essential to do so, for example to confirm your qualification achievement with the SIA. We aim to do so on the basis of your explicit consent unless there is a legal basis not to inform you, for example, where informing you would contravene money laundering legislation.

Personal data held for equal opportunities monitoring purposes

Where personal data obtained is to be held for equal opportunities monitoring purposes, all such data will be made anonymous.

Why do we process your data?

When we ask you to supply us with personal data we will make it clear whether the personal data we are asking for must be supplied so that we can provide the products and services to you, or whether the supply of any personal data we ask for is optional.

Contract performance

To take steps to fulfil or linked to a contract:

- To provide products and/or services which we are contractually obliged to provide to you, your client or the organisation you work for in relation to the contract;
- To keep you up to date with any information required in relation to contracted products and/or services between us;
- To discharge our duties as an employer.

Legal obligations / Public interest

- To fulfil any regulatory or statutory obligations of the organisation, such as to provide information or respond to any lawful or proportionate request by government authorities, law enforcement or statutory bodies,
- To keep basic records of your membership with us and any achievements or contributions to the administrative management field.

Vital interests of the data subject

- To protect the safety and security of yourself or others as outlined within our Safeguarding Policy or Health and Safety Policy.

Overriding legitimate interests

These interests may include our, or a third party's, interests. For example:

- For the purposes of good governance,
- To audit, analyse and protect systems and data from misuse,
- To maintain security, functionality and improve your experience on our website,
- To improve or develop our products and/or services,
- To monitor, analyse, and improve sales, organisational performance and business performance,
- To request for your consent to be contacted by us about relevant products / services,
- To conduct research relevant to Administrative Management, or our products / services,
- To ensure that members meet the criteria for membership,
- To collect outstanding debt owed to us,
- To resolve arising issues, complaints, claims, or disputes between us and you.

Consent

We will rely on your consent to:

- provide marketing or information which is not directly relevant to your contract with us,
- process or transfer sensitive information where it is not required by a legal, public interest or overriding legitimate interest obligation.

Marketing preferences

Each marketing email that is sent provides you with the ability to unsubscribe from receiving marketing emails at any time. Alternatively, you can change your preferences by sending a request to marketing@instam.org.

Automated decision making

The IAM does not currently process data by means of 'automated decision making' as defined by the GDPR.

IAM may from time to time promote / provide information on social media websites such as LinkedIn, and Facebook that may conduct 'automated decision making' in relation to our communication notices we post on those sites. Your interactions with us on those platforms are subject to the terms and conditions of the respective sites, and you do so at your own risk.

IAM aims to track your engagement with us on the site in which it originates and limit the transference of information outside of those sites in accordance with best practice and the terms and conditions of those sites. We will not store or transfer your interaction within those sites outside of the relevant social media unless there is a proportionate and necessary legal basis for processing. If you have any concerns about how your information is used and the notifications you receive on those sites, you are advised to contact them directly.

Sharing with third parties

We may disclose and share your personal information with:

- employers, education institutions or parent/carer (where they have purchased access to our products / services on your behalf)
- our service providers / contractors (for example, suppliers who develop or host our IT Services) to the extent where it is required to deliver products / services to you, or to uphold any overriding legitimate interest,
- external auditors, to the extent where it is necessary to assess our governance and compliance arrangements,
- law enforcement agencies, statutory organisations, governmental bodies or other relevant organisations where we have a legal or public interest obligation to do so,
- investigatory and fraud protection agencies, to verify your identity, prevent fraud and/or other criminal offences,
- to anyone we deem necessary to protect your vital interests, including the security / safety of yourself and / or other persons, as consistent with applicable law,
- debt collection agencies, to protect our legitimate business interests, (for example to collect outstanding debt from your organisation),
- an acquiring entity, in connection with a sale, joint venture or other transfer of some or all of our company or assets (subject to the commitment of the acquiring entity to comply with this policy),
- third parties in other situations with your consent.

Statutory bodies and government agencies we work with may include, but is not limited to, Her Majesty's Revenue and Customs (HMRC), Department for Work and Pensions (DWP), Institute for Apprenticeships (IfA), ActionFraud, Serious Fraud Office (SFO), Health and Safety Executive (HSE), Information Commissioner's Office (ICO).

All of our service providers, partners, and contractors are contractually required to implement appropriate technical and organisational measures to meet the requirements of applicable law, and to process information only in compliance with it.

International transfers

IAM also operate a number of international partnerships and have customers outside the European Union. Data originating from these regions may be processed in the UK and transferred back to its origin country. Data originating from the European Union will not be processed outside the European Union unless it is essential, and even so, not without adequate technical and organisational safeguards.

Whistleblowing and malpractice

In accordance with the conditions of recognition, we may report to third parties such as other membership organisations and statutory bodies where we have reasonable grounds for suspecting that you have committed a relevant criminal offence.

We will only share your information with organisations so far as is reasonable to investigate any allegations that may affect the delivery of our products / services, or to fulfil our legal obligations under any conditions of recognition applied by a statutory body.

Your responsibility

To protect personal information, you are urged to:

- notify us of any changes to your information / status to ensure your information is accurate and up to date,
- keep passwords safe,
- only access our services using secure networks,
- maintain updated internet security and virus protection software on your devices and computer systems,
- contact us immediately if you suspect a security or privacy concern or issue.

We may immediately suspend or terminate your access without notice if we become aware that you are in breach of our Terms and Conditions or of this Policy.

Confirming your membership to third parties

Save for the provisions under this policy and any legal obligation (such as court orders), we will not confirm your achievements to third parties without your consent.

We encourage verification requests to be submitted with the learner's or member's written consent.

If we receive a verification request stating:

- IAM members: your full name, date of birth, IAM membership number and IAM membership renewal date, (or a copy of the certificate / IAM membership card with those details)
- IAM qualification: your full name, date of birth, certificate number, and date of achievement, (or a copy of the certificate accompanied with those details)

We may confirm to a third party that membership / qualification that the details are correct and can be verified should all the details provide an exact match. If there is a discrepancy, we will only state that the information cannot be verified. We will not provide any further information about the discrepancy of information, and request that the third party contact you to submit a verification consent form.

In some cases of minor discrepancies, we may inform you that a verification request had been made, and ask you to confirm if you are happy for your membership or qualification details to be confirmed. If you cannot be contacted (either because you are no longer a member, or we do not have contact details about you), we will state that the information cannot be completely verified.

We will also not provide any other personal information and / or contact details about any member to a third party (save for our legal obligations to do so), although we may elect to pass on a message where we felt it was in your interest.

It is important that you keep your membership certificate, membership card and relevant numbers safe, and that you do not disclose these details to third parties if you do not wish for them to verify your details. By providing this information to a third party, you are consenting for the person to verify your membership / qualification status through any verification service which we operate.

Purposes for which personal data may be held (employees)

Personal data relating to employees may be collected primarily for the purposes of:

- recruitment, promotion, training, redeployment, and/or career development;
- administration and payment of wages and sick pay;
- calculation of certain benefits including pensions;
- disciplinary or performance management purposes;
- performance review;
- recording of communication with employees/students and their representatives;
- compliance with legislation;
- provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers; and
- Staff, volunteers and students, staffing levels and career planning.

Training

All IAM employees, partners and relevant contractors are required to keep up to date with training and updates provided by the ICO regularly for advice and guidance on data protection issues and to aid CPD. Unauthorised access, amendment, deletion or transfer of records will be treated as gross misconduct / malpractice by IAM.

Exercising your data rights

We aim to deal with any concerns which you may have about your information effectively and efficiently as part of our day to day operations with you.

If you have a concern about the way your data is used which cannot be addressed by the IAM Membership Executive, write to dataprotection@instam.org with your concerns or formally exercise your legal rights by using the Data Rights Form (instam.org/pdf/privacy/data-rights-form.docx).

The form covers the following requests:

- subject access request (SAR)
- amendment / rectification request
- object processing
- restrict processing
- erasure
- data portability

We won't normally charge a fee unless it was reasonable and within the confines of the law.

For more information about how your rights apply, please see the ICO guidance at ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

We aim to respect your request wherever possible however, please note that there are exception to when these rights may apply. If we are unable to comply with your request due to an exception, we will explain this to you in our response.

In some circumstances we may anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

We will usually comply with your request within 30 days of the receipt of your request, or at most, 60 days, if the information we hold about you is excessive.

Event of a breach

In the event of a breach of your personal information, we will take reasonable steps to inform you wherever possible. We will also make best endeavours to inform the ICO within 72 hours of first finding the breach.

Our recovery time objective (RTO) is:

- 1 working day for minor breaches
- 5 working days for serious breaches

This may be longer in serious or complex cases.

Retention of records

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any regulatory duty, public interest, or overriding legitimate interest.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

For example:

- Credit card information is not stored, such information is processed directly on PCI DSS Compliant systems provided by payment / banking providers.
- Summary member information and any recognition or contributions you have made to the Institute is normally held indefinitely as it is in both your and the public interest to be able to verify your membership and awards.
- Most personal information (including contact details, and CPD records) are deleted within 3 years of the termination of your membership.

For more information, please refer to the IAM's Data Retention Policy.

How we process your information

Process	What data do we collect / process	Fields with Personal Data	Why do we collect / process the data?	Legal basis for collecting	What System / where exactly do we store the data?	Do we send the data to someone else as part of processing?	How long do we retain it?
IAM Council Member appointment	Council members	Membership number, Member full name, DOB, Address, Email address, Telephone, Previous Membership numbers, CV/resume, references	To gather sufficient information to assess suitability.	Legitimate interest, contract performance	Microsoft Office 365	No	Length of appointment, plus 12 months
Website access	Website visitors (unauthenticated)	IP Address, Device details?	To monitor volumes of traffic	Legitimate interest	Website (Analytics)	No	Personal data not recorded
Marketing - IAM members	Newsletter subscribers	Member full name, email address,	To provide members with information as part of their benefits.	Legitimate interest	Microsoft Office 365, Mailchimp	No	Length of appointment, plus 6 months
Marketing – non-members	Consenting non-members	Full name, email address,	To provide non-members specific news and information of interest.	Consent	Microsoft Office 365, Mailchimp	No	Length of appointment, plus 3 months
New member / renewal process	Members	Membership number, Member full name, DOB, Address, Email address, Telephone, Previous Membership numbers, CV/resume	To gather sufficient information to assess correct membership level. To gather data to send out physical membership items – certificate, card, etc.	Legitimate interest, contract performance	Microsoft Office 365, Membership Portal (Plomino database), Dropbox	No	Length of appointment, plus 3 years

Payment processor (Stripe)	Collect personal information including Debit/Credit card details for payments	Membership Number, Full name, Address, Phone (Fixed/Mobile), Email address, Debit/Credit card details	To take the correct payment	Legitimate interest, contract performance	Web browser Stripe, Email, Dropbox	Yes, Stripe	Bank details are only for the length of the transaction. Record of the transaction, minus the bank details is 7 years.
Payment processor (GoCardless)	Collect personal information including Bank details for payments	Membership Number, Full name, Address, Phone (Fixed/Mobile), Email address, Debit/Credit card details	To take the correct payment	Legitimate interest, contract performance	Web browser GoCardless, Email, Dropbox	Yes, GoCardless	Bank details are only for the length of the transaction. Record of the transaction, minus the bank details is 7 years.
Payment processor (Worldpay)	Collect personal information including Bank details for payments	Membership Number, Full name, Address, Phone (Fixed/Mobile), Email address, Debit/Credit card details	To take the correct payment	Legitimate interest, contract performance	Web browser Worldpay, Email, Dropbox	Yes, Worldpay	Bank details are only for the length of the transaction. Record of the transaction, minus the bank details is 7 years.
New/renewal member process - invoicing	Member personal details for requesting Membership payments	Full name, Address	Audit trail for payments. Keep accurate and up-to-date financial records.	Legitimate interest, contract performance	Microsoft Office 365, Email, Dropbox	No	Length of appointment, plus 7 years.
CPD documentation	Members can complete CPD information and claim certificates once they score a minimum number of points	IAM Membership Number, Full name, Email, (other personal information)	Keep accurate and up-to-date member records.	Legitimate interest, contract performance	Microsoft Office 365 Membership Portal (Plomino database), Dropbox	No	Length of appointment, plus 3 years
Shop (e-commerce)	Both members and non-members are allowed to make purchases for events, conferences, certificates	IAM Membership Number, Full name, Address, Email address	Audit trail for payments. Keep accurate and up-to-date financial records.	Legitimate interest, contract performance	Microsoft Office 365 Membership Portal (Plomino database)	No	Bank details are only for the length of the transaction. Record of the transaction, minus the bank details is 7 years.

Complaints

We take very seriously any improper collection or misuse of personal information. Please report it to our Data Protection Officer at dataprotection@instam.org.

You can also complain to us by contacting the General Manager directly.

If you believe that your data protection rights may have been breached, and we have been unable to resolve your concern, you may lodge a complaint the applicable supervisory authority or to seek a remedy through the courts. Please visit ico.org.uk/concerns/ for more information on how to report a concern to the UK Information Commissioner's Office.

Signed: **Date:**

Chief Executive