imparta®

Information and Personal Data Security at Imparta

REVISED: 12/11/2024

Table of Contents

Overview of Operations

The secure handling and processing of personal data is a high priority at Imparta. This document provides an overview of the actions and processes we have put in place to protect your personal data and confidential materials and ensure the security of our networks, systems and platforms.

Imparta Ltd. is a sales and customer service training company with offices in the UK (United Kingdom) and a 100% owned subsidiary, Imparta Inc. in the USA. The information provided in this document applies to the shared information systems of both Imparta Ltd and Imparta Inc.

Personal data is processed to provide Imparta's clients with training and related activities, including, but not limited to, workshops, coaching, assessments, training reinforcement and online learning.

Personal data is held on two Microsoft systems, i-Coach and Microsoft 365. i-Coach is Imparta's proprietary web-based learning management platform which is hosted on Microsoft's cloud-based Azure platform. The Azure platform plays a central role in the provision of online learning, the organisation of training workshops, and other training related activities.

Imparta's internal data infrastructure runs on Microsoft 365 – which in turn is hosted on Microsoft Azure infrastructure – for the day-to-day management of client activities that take place outside i-Coach, for example, storing personal data provided by clients in client folders. These activities take place on SharePoint and Microsoft Teams, both part of the Microsoft 365 suite. Confidential materials shared by the client may also be stored on Microsoft 365. Microsoft Teams is used for the secure sharing and transfer of personal data unless a client requests an alternative secure transfer and sharing platform.

Security Governance

INFORMATION SECURITY MANAGEMENT SYSTEM

Imparta's Information Security Management System (ISMS) helps us manage the overall security infrastructure and polices at Imparta. The ISMS includes policies, procedures, and standards that define the controls that help support the confidentiality, integrity, and availability of the Imparta services. Additionally, the ISMS outlines the roles and responsibilities of employees at Imparta to help protect the confidentiality, integrity, and availability of Imparta's services.

INFORMATION SECURITY REVIEW BOARD

The ISMS Review Board oversees the Information Security Management System. The Board includes members of Imparta's Senior Executive Team and managers with responsibility for operation of ISMS processes.

The Review Board meets at least quarterly. The Review Board's responsibilities include:

- Overseeing security policies and procedures, including implementation and updates
- Overseeing security risk assessments and audits
- Third party processor reviews
- Monitoring compliance with the Information Security Management System

Imparta is ISO 27001 accredited. Imparta's annual ISO 27001 accreditation is overseen by the ISMS Review Board and an annual audit carried out by a third party.

A copy of Imparta's current ISO 27001 certificate is available in Annex A.

Data hosting and Location of Processing

LOCATION OF DATA HOSTING AND PROCESSING

Imparta use databases that logically store personal data and organise other components for quick retrieval and faster processing.

Personal data on i-Coach can be held in the EU or USA on Microsoft Azure at the client's direction. However, processing of personal data on i-Coach will take place in the UK and any other locations requested by the client and where the necessary agreements, for example EU Standard Contractual Clauses, are in place.

Personal data held within Microsoft 365 is held in the UK. Personal data may be processed in the EU, USA or other locations dependant on the location of the client and the training activities being carried out and again where the necessary contractual agreements are in place.

Personal data may be transferred and processed outside the data centre or processing region to comply with Customer requests or as strictly necessary to provide the training services instructed.

Imparta only processes personal data to the extent necessary to provide i-Coach and requested training services and in accordance with our contractual arrangements and does not disclose any personal data to third parties other than in accordance with applicable law or any contractual agreements or client request.

Imparta has key operations in the following locations:

FUNCTION	DESCRIPTION
i-Coach data centres	i-Coach is hosted on Microsoft's cloud-based Azure platform. The data centres are located in the following regions: • Europe (Netherlands and Ireland) • US (Virginia) Clients can decide whether personal data on i-Coach should be stored on Azure in the US or the EU.
Operations data centres	Imparta's operations are hosted on Microsoft 365, with data locations in the UK.
Client support	Client support teams operate out of the UK and US depending on project location. Zendesk is deployed for i-Coach support ticketing. Any personal data provided to Zendesk is provided directly by i-Coach users and held in the EU (Dublin).
System engineering	The systems engineering and software development teams are located in the UK

Microsoft Security

Azure is trusted by over half a million organisations. If you'd like to learn more about Azure security practices, please check out these links:

- ISO Global Certification for Microsoft 365
- ISO Global Certification for Azure
- Overview of Security Processes
- Service Organization Controls Report
- Azure Customer Case Studies

We use many Azure-provided solutions including relational databases, full-text search, queuing, messaging, identity management, encryption, and caching. As part of our business continuity plans in case of disaster, we practice automated, routine, and frequent data backup and recovery. We aim to eliminate single points of failure in our infrastructure and have built redundancy into all our services. All Imparta services are redundant across two or more physically isolated and resource-independent availability zones in Europe. This ensures multiple data centres can go offline simultaneously whilst we continue to provide customers with a full service.

People

The following teams support Imparta's platforms and systems:

ROLE	RESPONSIBILITIES
i-Coach Support	Online and email support for i-Coach
Project Management	Client support and project management
Information Security	Corporate Infrastructure Corporate Wireless Networks Workstation Management ISO 27001 Compliance Penetration Testing Vulnerability Management Security Alerting and Monitoring Intrusion Detection Security Awareness Training Incident Response
System Engineers	New Code Development Configuration Standards Quality Control and Fixes Performance Monitoring
Platform Security	i-Coach Penetration Testing i-Coach Vulnerability Management i-Coach Security Alerting and Management i-Coach Intrusion Detection i-Coach Incident Response
People Operations	Employee Onboarding/Offboarding
Chief Information Officer	Contracting Privacy Data Compliance Data Security Training

Policies and Procedures

Imparta is ISO 27001 certified and implements and reviews all ISO27001 controls through Imparta's Information Security Management System. ISO 27001 includes controls on:

- Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System acquisition, development, and maintenance
- Supplier relationships
- Information Security Incident Management
- Business Continuity Management
- Compliance.

Control Environment

Imparta's dedication to excellence is driven from the top of the organisation. Executive management emphasises the importance of well-designed and operated security controls through the ISMS Board. Management takes seriously any control deficiencies identified in internal and/or external audit reports and takes full responsibility for remediation activities.

Risk Management

Imparta's risk management approach is detailed in the ISMS. The Executive Team have responsibility for overseeing risk management within the Company as a whole. The Executive team carry out this responsibility through the ISMS Review Board.

The senior management team supports, advises and implements policies approved by the Board and officers.

Management recognises and weighs the financial and non-financial implications of the risks. Managers are responsible for encouraging good risk management practice within their department(s).

Key risk indicators are identified and closely monitored on a regular basis through the ISMS.

RISK ASSESSMENT

Internal ongoing audit activities are performed continuously by members of the ISMS Review Board to identify, manage, and respond to risks to the organisation, and there is a full internal review of all controls every year before the annual ISO recertification.

The assessment process is based on the ISMS Risk Framework where threats and risks are assessed on a grid measuring likelihood and impact of the risk.

All risks are managed using a risk treatment plan, where appropriate controls are identified to keep risks within acceptable risk levels.

INTERNAL AND EXTERNAL AUDIT

Internal audits are an important element of maintaining an effective control environment. The program is comprised of several members from various teams, including finance, software development, information security, and the Data Protection Officer. At least annually, there is a full review of the effectiveness of all critical internal controls.

External auditing is performed by an independent, accredited body on an annual basis. Full recertification is done every 3 years, with surveillance audits carried out annually.

Any findings coming out of audits are collated into remediation plans. These plans are presented to the ISMS review board and actioned according to urgency.

Asset Management

INVENTORY OF ASSETS

An inventory of all computing devices is continuously maintained, with periodic spot checks to confirm the location and current ownership of all systems.

ASSET OWNERSHIP

Assets are assigned to owners, who then assume responsibility for the asset under their control. All assets are controlled and maintained by the IT department, who ensure that all computing devices are kept up to date and safe from malicious actors.

BASELINE HARDENING STANDARDS

Systems are configured centrally, with a baseline image applied to all devices, and conform to the requirements of a modern IT infrastructure. Updates are applied to all devices, with automated reporting on any devices that fall out of scope. The security defaults being applied to all machines conform with CISA baselines.

TIME SYNCHRONISATION

Device clocks are synchronised using public NTP servers to ensure all devices are keeping time correctly.

Business Continuity and Disaster Recovery

The organisation's primary goal is to deliver services to its clients, and all effort will be put into maintaining these services and to restore them as quickly as possible in the event of an event interrupting this service.

Imparta has a business continuity plan (BCP) to ensure appropriate actions are taken in the event of a disaster. The purpose of this business continuity plan is to ensure prompt and complete return to normalcy in the event of a service-affecting disaster. The plan details actions to be taken by certain individuals in the business, as well as outlaying which teams would be responsible for which actions.

The BCP details which communications are issued by which members of staff, both for internal and external communications.

The BCP is tested annually to ensure that it is effective and relevant.

The BCP includes a disaster recovery plan (DRP). This plan ensures that the relevant teams have all the necessary information at hand to ensure a prompt return to operations. An escalation plan is put in place to ensure all executive team members are alerted when a disaster occurs.

In the event of a communications system failure, all team leaders have alternate contact details for their immediate reports, and vice versa. Customer representatives will be notified by their dedicated client team through email or telephone.

The expected return to operations (RTO) for any issues with the client-facing web applications is 24 hours. Any systems outside of our control are expected to RTO within the SLAs (service level agreements) set in the contracts we have with these providers.

Change Management

We operate a formal change management process to ensure changes to the production environment don't affect operations.

The IT department operates a change management system where any changes need to be pre-approved by the Head of IT. Any changes are to be detailed in the change management log. The log details rollback procedures and a testing regime, as well as the engineer responsible for the change. Any further detail about the change is to be logged separately in a document in the same folder, linked to the change ID by means of having the same name as the ID.

DEVELOPMENT METHODOLOGY

The development team also operates a change management procedure where any changes need to be pre-approved by the Head of Software Development. All development and testing activities take place outside the live environment. Any changes to the program code or the system database are logged in Azure DevOps with the specific projects via project tasks, bugs and work items which are needed before any work is undertaken. Specific change sets are logged by specific development users and the system traces all code repository updates.

The configured build and deployment pipelines are logged and stored so that the system can be rolled back to specific stages or to any point in time.

Personal Data Management

All personal data is owned and controlled by Imparta's clients, who are designated as data controllers. Imparta is the data processor. Clients determine the following about the personal data:

- Which type of personal data to collect
- Who to collect personal data from
- When and how to amend personal data
- Where to collect personal data
- What purpose to use the personal date for
- When to delete the personal data

There are several personal data types that Imparta collect, and each type generally falls into one of the following categories:

Participant Data: Personal data collected to enable the implementation of training and training related activities. This will typically include names of participants in the training, and their business email addresses. It may also include organisational information such as business unit and geographical location and the reporting hierarchy of participants.

Progress Data: Personal data collected that collates and reports on a participants progress in training activities, for example attendance in workshops, progress in online learning, and assessments completed. This will be viewable in reports for nominated client administrators, either directly through I-Coach or as provided directly by the project team.

User Information: The requisite username (User login ID) and password for logging into the i-Coach platform. Passwords cannot be viewed by system administrators. All logins are logged.

THIRD PARTY PROCESSORS

Imparta use the minimum number of data processors necessary to achieve our clients' training objectives and provide our training services. Microsoft services are fundamental to Imparta's ability to provide the training services our clients require. Zendesk is required if a client is using i-Coach and an i-Coach user (client employee) has a support enquiry. Qualtrics is deployed where clients request participant feedback and other impact surveys to be carried out.

Imparta's trainers are often third parties accredited to deliver Imparta training. These trainers have limited access to personal data, typically the names and emails addresses of participants on a training event they are delivering. This data is provided to them securely on i-Coach.

LIST OF THIRD-PARTY PROCESSORS

NAME OF PROCESSOR	PURPOSE OF PROCESSING	BUSINESS ADDRESS	LOCATION OF DATA PROCESSING
Microsoft Azure	Hosting of i-Coach	Microsoft Inc., Thames Valley Park; Reading; RG6 1WG.	EU (US option on request) and UK
Microsoft 365	SaaS productivity platform for handling Imparta communications and file storage	Microsoft Inc., Thames Valley Park; Reading; RG6 1WG	UK
Imparta Ltd (100% owner of Imparta Inc.)	Customer and service support and administration and operation of i-Coach learning platform	Imparta Ltd, 522-524 Fulham Broadway, London SW6 3BN	UK
Zendesk	Ticketing and management of support enquiries received through i-Coach	989 Market St San Francisco, CA 94103	EU (Ireland)
Qualtrics (optional)	Surveys and analysis for sales training impact assessments	Qualtrics UK Headquarters 10 York Road	EU (Frankfurt)

NAME OF PROCESSOR	PURPOSE OF PROCESSING	BUSINESS ADDRESS	LOCATION OF DATA PROCESSING
		Waterloo, London SE1 7ND England	
Imparta Inc.	100% owned Imparta subisdiary–For providing support for US projects and the provision of extended out of hours support for other regions.	954 Lexington Ave. #1081, New York, NY 10021	US

THIRD PARTY PROCESSOR DUE DILIGENCE

To help mitigate risk to Imparta and our clients, the ISMS Review Board performs reviews of third-party processors, and the services they provide. The assessment process evaluates suppliers' security and data handling standards and security accreditations and is based on responses and evidence provided by the supplier. Control areas reviewed include, but are not limited to, information and systems security, network security, general security (including physical security), vulnerability management, incident response, data security, accreditations, and data privacy.

The Imparta contracts team ensures information security and regulatory requirements are captured as part of service level agreements with third party processors.

ENCRYPTION OF DATA IN TRANSIT

All data is encrypted in transit whether through Microsoft Teams, email or SharePoint. Staff can classify data as "Confidential" or "Personally Identifiable Information".

All transfers use a 2048 bit RSA key. Key material is signed using SHA-256 with RSA Encryption.

For connection to our cloud-based document and file services:

Transfers use elliptic curve cryptography, a 256 bit key with a 256 bit base point order length. Key material is signed using SHA-256 with RSA Encryption

ENCRYPTION OF DATA AT REST

All our data is encrypted at rest using AES 256-bit encryption. AES is an encryption protocol which uses a key length of 256 bits. AES has become the gold standard for encryption due to its robust protection against brute force attacks.

ENCRYPTION KEY MANAGEMENT

All encryption keys in use by Imparta are stored on Azure Key Vault.

ENCRYPTED BACKUPS

All backups are encrypted at rest using AES 256-bit encryption.

DATA USED IN TEST ENVIRONMENTS

Client data is never used in the i-Coach test environment. We utilise a separate testing environment which is identical to the production environment, though it does not contain any client data.

DATA DELETION

Personal data is anonymised or beyond use at the request of a client within 48 hours. Personal data in i-Coach is anonymised and cannot be reconstituted. Any personal data in Microsoft 365 (SharePoint) is put first beyond use and then deleted permanently in line with Imparta's retention schedules. If a client does not request deletion of personal data at the end of a project, Imparta will anonymise (i-Coach) and put beyond use and then delete (Microsoft 365) the personal data 12 months after the last invoice date or revenue recognition activity. Securely held backup copies are deleted in line with Imparta's retention schedule.

BACKUP MANAGEMENT AND RETENTION

For our internal infrastructure – hosted at Microsoft 365 – backups are taken automatically every 8 hours and stored in an online location separate from our 'in use' principle data centres. Backups and snapshots are kept in line with our backup retention schedule which will not be longer than one year.

Our i-Coach environment is web based, and backups of the source code are stored in-line within the DevOps environment. I-Coach backups are maintained for six months.

The SQL database is backed up in its entirety via the MS Azure environment.

DISPOSAL OF MEDIA

Formal processes and procedures are in place to securely dispose of devices that may contain personal data. These procedures apply to all data center environments. Deprecated or defective media (specifically, hard drives) are erased using a 3-pass overwrite procedure, and the disks are safely stored and held until enough disks have been collected to be collectively destroyed by a third-party data destruction company.

Endpoint Protection

All devices owned and operated by Imparta are managed by a centralised device management system which enforces the application of rules designed to secure the devices against any misuse or malware infection.

Software applications are limited to only those that are required for business needs. End-users cannot install software unless previously authorised by the Head of IT after a risk assessment. Installs are performed by IT staff using elevated privilege accounts.

We use a centralised device management solution to enforce policies across all client devices. These policies include disk encryption, security defaults, automatic updates, clock synchronisation, automatic screen locks.

All system disks are encrypted using BitLocker. Any external disks inserted into the devices will automatically be encrypted in order to be accessible.

A clean desk policy is in place in the main office, which means that any documents that are printed are to be destroyed if containing personal data, and none must be left unattended at any time. This is communicated to all staff during regular security training sessions.

All workstations are configured to automatically lock the screen after 10 minutes of inactivity.

A mobile device policy is in place that mandates an automatic lock and the requirement of a 6-digit PIN (Personal Identification Number) to unlock the device if it accesses company email. Devices are configured with location features enabled so they can be wiped remotely in the case of loss or theft.

General Operations

Imparta has contractual agreements in place with all clients that detail the contractual relationships between the client and Imparta. Personal data processing agreements are also in place with all Imparta clients.

The Imparta i-Coach online privacy statement details how Imparta processes personal information (https://www.i-coach.com/Info/PrivacyPolicy). In addition, the i-Coach Terms and Conditions (https://www.i-coach.com/Info/Terms) state the terms and conditions including acceptable user policies regarding I-Coach.

Imparta reserve the right to disable any User account on i-Coach suspected of violating the i-Coach Terms and Conditions.

CLIENT SUPPORT

Client Technical Support is supplied online through i-Coach. The i-Coach support team are operational during UK business hours and endeavour to answer all queries withing 24 hours. Imparta staff may ask for personal information before accessing an i-Coach User's account to confirm the User's identity. They will never ask for a user's password. Passwords are not viewable by any Imparta employee. With the User's permission, Imparta may access an account to support the User or diagnose a software problem. Each client's project team provides non-technical project support and can help liaise on any technical issues.

WEB PRACTICES

Imparta collects and analyses aggregate information of visitors to i-Coach and Imparta's website, www.Imparta.com, including the domain name, referring URLs, and other publicly available information. We use this information to help improve our services and customise our pages' content.

COOKIES

Cookies in i-Coach are used to maintain the session state, and do not include any response data or personal information. More information on cookie usage can be found in our Privacy Statement (https://www.i-coach.com/Info/PrivacyPolicy).

ANTI-CORRUPTION AND ANTI-BRIBERY

Imparta has a strict anti-bribery/anti-corruption internal policy to conduct all business ethically, not to send or receive bribes, or to otherwise take part in corrupt activities.

PROTECTING CHILDREN

Imparta does not knowingly collect personal information from children under 16 for any purpose.

INSURANCE

Imparta maintains A rated insurance for standard policies and coverages.

Identity and Access Management

ACCOUNT PROVISIONING

Imparta follows the principle of least access when assigning access rights to employees. All new Imparta staff receive training in data protection and IT security which is refreshed annually. All Imparta staff sign up to Imparta's security and data policies. Passwords are set by employees and accounts cannot be accessed by other staff members. Sharing of account details is expressly forbidden in the employee handbook and this policy is reinforced through training. Staff will only be given access to the client folders on Microsoft 365 which are relevant to their duties.

TERMINATION: ACCOUNT DE-PROVISIONING

When an employee terminates their employment, a workflow is activated on Imparta's HR system informing the IT Team of the leaving date and the necessary steps to de-register the user account. This includes information on what to do with email access, email forwarding to the appropriate team member, security group membership, distribution list membership and software license removal.

ACCESS AUTHENTICATION

Access to the i-Coach production environment is managed through multiple network and authentication layers using numerous usernames, passwords, and multi-factor authentication (MFA) tokens.

Access to the production infrastructure is restricted to authorised personnel based on job function. Privileged system access is restricted to a limited number of system administrators.

PASSWORD POLICY

The password policy for privileged accounts on production systems are required to meet the following password parameters:

- Passwords must be a minimum password complexity of 8 characters and must contain a combination of letters, numbers, and symbols based on available system functionality.
- Password maximum lifetime is restricted to 6 months.
- Passwords cannot be reused for at least 16 generations.
- Account lockout settings are enforced after a number of consecutive invalid login attempts and automatically lock the account after the number of unsuccessful attempts is exceeded.

For i-Coach, user passwords are managed directly on the system or through SSO on the client's directory. Passwords on i-Coach are required to meet the following password parameters:

- Password complexity can be configured on a client-by-client basis.

- Default passwords must be a minimum password complexity of 8 characters and must contain a combination of letters, numbers, and symbols based on available system functionality.
- Default password maximum lifetime is restricted to 3 months.
- Account lockout settings are enforced after a number of consecutive invalid login attempts and automatically lock the account after the number of unsuccessful attempts is exceeded.

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is enforced on all accounts and is required to access company applications (e.g., email, internal systems, sales software). Re-authentication is required every 30 days or whenever there is a request to access company applications from another source.

SECRET STORAGE

Secrets (including cryptographic keys and passwords) for i-Coach and Imparta's networks are stored in a security vault system. Access is restricted based on the principle of least privilege and limited to authorised personnel only. Secrets are rotated periodically.

INCIDENT RESPONSE

Imparta has an incident response tracking system built into the ISMS. The procedures for incident response planning are defined in advance of an incident occurring and have been agreed by the ISMS Review Board. The Security Incident Management tracker guides an incident through the key states it needs to go through ensuring that all incidents receive the same structured approach. These are:

The item on the track is used to track all work relating to the investigation and resolution of that incident. If further work is needed a project to track that work will be created and linked to that track item.

DATA BREACH NOTIFICATION REQUIREMENTS

Where a security incident is suspected or confirmed to have affected personal data, the Data Protection Officer will be informed at the earliest opportunity and the Data Protection Officer will take responsibility for any GDPR compliance requirements.

Staff are trained on reporting information security events and reporting information security weaknesses.

Network Operations

DATA FLOW

Data flow diagrams are available in Annex B of this document.

WIRELESS NETWORKS

In Imparta's headquarters, a corporate network is set up to allow all corporate devices to connect wirelessly. All devices are centrally configured to automatically connect based on their security profile, and the network cannot be connected to using a username and password.

For guest access, a separate SSID is available. This connection issues unique IP addresses on separate subnets for each connection, so no devices can see each other on this network.

VPN CONNECTIONS

Imparta staff and associate faculty members have access to the company VPN system to ensure encrypted connections at all times.

Traffic is encrypted using AES-256 and 3DES-168 and SSO with MFA is enforced.

People Operations

Imparta's commitment to client service requires the hiring of the best talent. All new hires are held to rigorous standards and undergo comprehensive assessment tests and competency-based interviews. Imparta also carries out employment verification and criminal record checks where allowed by law, Imparta is an equal opportunity employer.

EMPLOYMENT AGREEMENTS

Upon hire, all Imparta employees are required to sign an employment agreement containing privacy and confidentiality obligations that specifically address the risks of dealing with confidential information, including personal data and information security. Any employee found to have violated this policy will face disciplinary action.

DISCIPLINARY PROCESS

Employees alleged to have violated Imparta's information security policies are investigated. Depending on the severity of the allegations and results of the investigation, Imparta may suspend the employee and withdraw access to Imparta networks. Following the investigation, notification occurs to the appropriate internal parties regarding results of the investigation and any disciplinary actions taken.

Corporate Office

SECURED FACILITY

Imparta's Head Office in in central London. Imparta staff work both in office, and remotely as determined by company policy and manager discretion. No data servers are located on Imparta premises as all data and IT operations are hosted in the cloud. The only equipment on site is for local internet connectivity facility, and this is not considered part of the critical infrastructure.

Imparta's Head Office is secured using access passes assigned to individual employees and access is monitored. No unauthorised persons can access the building without prior permission.

VISITOR ACCESS

Visitors are signed into the visitors' book and are always accompanied by an authorised person. Visitors must sign out when leaving the premises.

Systems Monitoring

SECURITY MONITORING

Production systems are configured to automatically log events such as logon events, account management events, elevated privilege functions, and other system events. Automated reports are sent to the IIT team, informing the team of any security incidents in real time. Corrective action is undertaken depending on the severity of the event and tracked using the corrective actions tracker.

INTRUSION DETECTION

We utilise Microsoft Defender as a first line of defence, and we use Microsoft Threat Intelligence to detect and report on intrusion attempts.

PERFORMANCE MONITORING

Automated reports are sent to the admin team to report on performance issues. The system is monitored continuously for any events impacting performance of the platform. System capacity is continuously monitored and reported on in regular ISMS Review Board meetings.

LOG RETENTION AND PROTECTION

Microsoft 365 logs are retained for 10 years and cannot be altered by anyone, including by global administrators.

Training and Awareness

GENERAL SECURITY AND PRIVACY AWARENESS TRAINING

Imparta employees are formally trained on company policies and security practices both on hiring and throughout their time with Imparta. This training occurs at least annually through in-person and online training. A security test must be passed each year by all employees. In addition to the in-person trainings, regular updates are provided throughout the year through email, and regular company meetings. All employees are instructed to immediately report possible security incidents to their manager, and the Head of Information Security. Imparta's employee handbook includes policies and guidance on the following topics:

- Privacy law compliance
- Physical security
- Email acceptable use policy
- Access control
- Internet security
- Personal devices in the Company
- Information Security Incidents
- Password policy and tips.

SECURITY TRAINING FOR ENGINEERS AND SOFTWARE DEVELOPMENT TEAM

All engineers and members of the software development team receive the general security and privacy awareness training. In addition to this, senior engineers receive training on management of the security aspects of the Azure Portal for i-Coach.

Members of the software development team are trained on how to access and manage the Azure SQL database that i-Coach uses. This training includes the restoring of database backups and the process of anonymising data for a specific client or User. This training is carried out on development copies of the database in Azure.

Engineers are also trained in how to securely deploy releases and hotfixes of the i-Coach system to development and also production environments. Training is provided in how to roll back a release to a previous version.

Vulnerability Management

VULNERABILITY ASSESSMENT, TRIAGE, AND RESOLUTION

Imparta has a robust vulnerability management system to ensure no vulnerabilities end up in the production environment. This is done through malware detection, patch management and regular penetration testing.

When vulnerabilities are detected, these are handled using our Corrective Actions & Improvements tracker and followed up until resolved. Corrective actions are based on the vulnerability's impact and likelihood assessment.

ANTI-MALWARE DETECTION

The use of anti-virus software on employee devices detects and eliminates the vast majority of common malware that is in existence. Imparta's end-user devices are all equipped with Microsoft Defender for Endpoint, which is centrally managed by the IT department, with automated reporting of detected threats.

We use malware scanning at the Exchange Online level through Advanced Threat Protection to minimise the risk that a user will encounter malware.

PATCH MANAGEMENT

Software patches are released on a regular basis, in line with Microsoft's monthly patch updates. Before deploying to the entire business, patches are released to a group of test machines and assessed for stability and functionality. Once approved, all patches are released to the rest of the business.

PENETRATION TESTING

Penetration testing is carried out annually for our Microsoft 365 environment.

i-Coach is tested on an ongoing basis using automated vulnerability testing. This system scans the development environment for known threats and configuration issues and reports automatically on any found vulnerabilities. A manual penetration test is carried out annually to complement the automated testing on i-Coach.

Artificial Intelligence

Artificial Intelligence (AI) is a powerful tool that will change, disrupt and, in many cases, improve how many of us work over the next years.

The Imparta IT policy instructs all employees to be very careful when using it. AI tools such as ChatGPT and CoPilot are developed through machine learning. Employees are instructed that they must not submit to any AI tool:

- Client personal data or client confidential information.
- Imparta personal data or client confidential information.
- Imparta intellectual property (including all forms of course materials).
- Any Imparta or client's software code.
- Anything owned by someone else.

Doing so will be a serious disciplinary offence.

Employees are also instructed to recognise AI's limitations and always use their judgment when interpreting and acting on AI-generated recommendations. AI systems are to augment human decision-making, not replace it.

IMPARTA I-COACH AI TOOLS

i-Coach AI is designed to work with multiple large language models (LLMs), including Microsoft's Azure OpenAI and OpenAI, as well as other LLMs. Microsoft's Azure Open AI is the default LLM used by i-Coach AI, although Imparta reserves the right to change the default LLM to an alternative provider such as OpenAI. If it does so, Imparta will use an alternative provider which is reputable within the industry and has reasonably comprehensive security arrangements in place. In addition, clients may request i-Coach AI to operate through alternative LLMs or their own LLM instances. In such cases, Imparta will not be responsible for the performance or security of those LLMs requested by clients. i-Coach and Microsoft's Azure OpenAI are both hosted on Microsoft Azure for processing and storage. i-Coach AI has been trained and prioritises content from Imparta's sales, coaching, customer experience and leadership programmes.

i-Coach AI provides:

- Text-based and voice-activated coaching at the point of need from an AI coach equipped with Imparta's intellectual property.
- AI call simulators and role-plays that allow salespeople to practise important sales and CX calls in advance.
- Insights and assistance when completing Imparta sales account planning tools (canvasses) within Salesforce and Microsoft Dynamics.

We can also incorporate client products and service information, along with specific sales expertise, into i-Coach. AI tools will soon include proactive call coaching within communication platforms such as Teams alongside AI call assessments, which leverage our competency models and add to our existing 180° skill assessments.

Clients may choose to deploy Imparta's i-Coach AI tools within i-Coach, or Salesforce or their own LMS or CRM depending on integration compatibility.

The AI tools do not require Personal Data to be input to access them. Users may, at times, input confidential information or personal data into i-Coach AI. If confidential information or personal data is input into i-Coach AI, the conversation should be deleted by the User. The stored conversation will not be accessible by third parties but will be stored on i-Coach and processed on the LLM, should the conversation be continued. If you input Client Confidential information into iCoach AI, for example, product information, this will also be processed by the LLM and i-Coach.

All AI features are clearly marked as AI, and the Terms and Conditions and Privacy Agreements detail how inputs and outputs are managed. The terms also make clear that AI has limitations, including but not limited to:

- Accuracy: AI algorithms are designed to analyse data and make predictions or recommendations, but they may not always be accurate or error-free. Users must exercise critical thinking and judgment when using i-Coach AI and not solely rely on it without verifying decisions or proposed actions through other sources.
- Bias: AI systems may inadvertently reflect biases in the training data. While we have used our reasonable endeavours to mitigate bias in i-Coach AI, you acknowledge and agree that its Outputs may not always be completely impartial.
- Unforeseen circumstances: AI models, including i-Coach AI, operate based on historical data and patterns. This means that i-Coach AI may struggle to predict outcomes in new or unforeseen situations.

We confirm to clients that the inputs and outputs are not available to third parties, including to other customers, are not used to improve open AI models automatically, and do not interact with any services operated by third parties outside of our managed secured cloud environment, including with Microsoft's Azure OpenAI Service. The only exception is if the client asks for inputs and outputs to be stored; these are stored and processed on i-Coach and on the Microsoft Azure Open AI platform. If inputs and outputs are not stored, they are deleted when the user logs out.

Integration with OpenAI ensures robust security through several key measures. Data transmitted between i-Coach and OpenAI is protected by end-to-end encryption, while Azure's comprehensive security infrastructure, including firewalls and DDoS protection, further safeguards these exchanges. Secure authentication mechanisms ensure that only authorised components can access OpenAI's APIs. Regular security audits and adherence to global standards like ISO 27001 and GDPR enhance our security. OpenAI's strict data privacy also maintains our services' confidentiality, integrity, and availability. i-Coach AI has been tested for accuracy, bias, unowned IP and offensive materials.

Using the i-Coach Learning Platform

Access to i-Coach is provided to clients employees (users) in two ways. A single sign (SSO) authentication scheme allows users to log in with a single ID linked to the client's internal learning management system or other network system. Alternatively, Imparta provides access to each User, and the User sets up their username (business email address) and password.

PASSWORD MANAGEMENT

Failed Attempts: To block unauthorised access through password guessing, accounts are disabled after three invalid login attempts. The account is blocked for one hour, and then the User can reset the password by contacting i-Coach support through i-Coach.

Password Complexity: A user's password must contain 8 characters, including at least one upper-case and lower-case letter, number and special character.

Password Expiration:

Forgotten Password Policy: If a user forgets their password there is a self-service password reset option that sends an email with a link to create a new password.

i-COACH SUPPORT

i-Coach Support is available between 9 am and 5:30 pm business hours on Monday to Friday except on UK bank holidays. Support enquiries are typically requests for help with passwords, or basic navigation requests. All requests are typically responded to within 24 hours during the working week, and basic requests also resolved within 24 hours.

Annex A

Imparta ISO 27001 certificate

CERTIFICATE OF REGISTRATION

PEERS QUALITY ASSURANCE LTD

This is to certify that

Imparta Limited (also trading as Imparta Inc.)

Of

522-524 Fulham Road, London, W6 5NR, United Kingdom

954 Lexington Avenue #1081, New York City, New York 10021, USA

Operates an Information Security Management System which has been assessed as conforming to:

ISO/IEC 27001:2022

For the Scope of activities:

Development & delivery of sales and customer experience training & Learning consultancy and associated learning applications for the Global marketplace.
Statement of Applicability Version 1

Certificate Number:	QEC/12/2541765347
Date of Initial Assessment:	23/05/2023
Date of Registration:	22/11/2022
Date Re-Issued:	17/10/2024
Date of Expiry:	21/11/2025

Certificate approved by:

Chris McMillan - Managing Director
Peers Quality Assurance Limited

This Certificate remains the property of
Peers Quality Assurance Limited
Suite 3, Rossway Business Centre
Wharf Approach
Aldridge
WS9 8BX England
www.pqal.co.uk

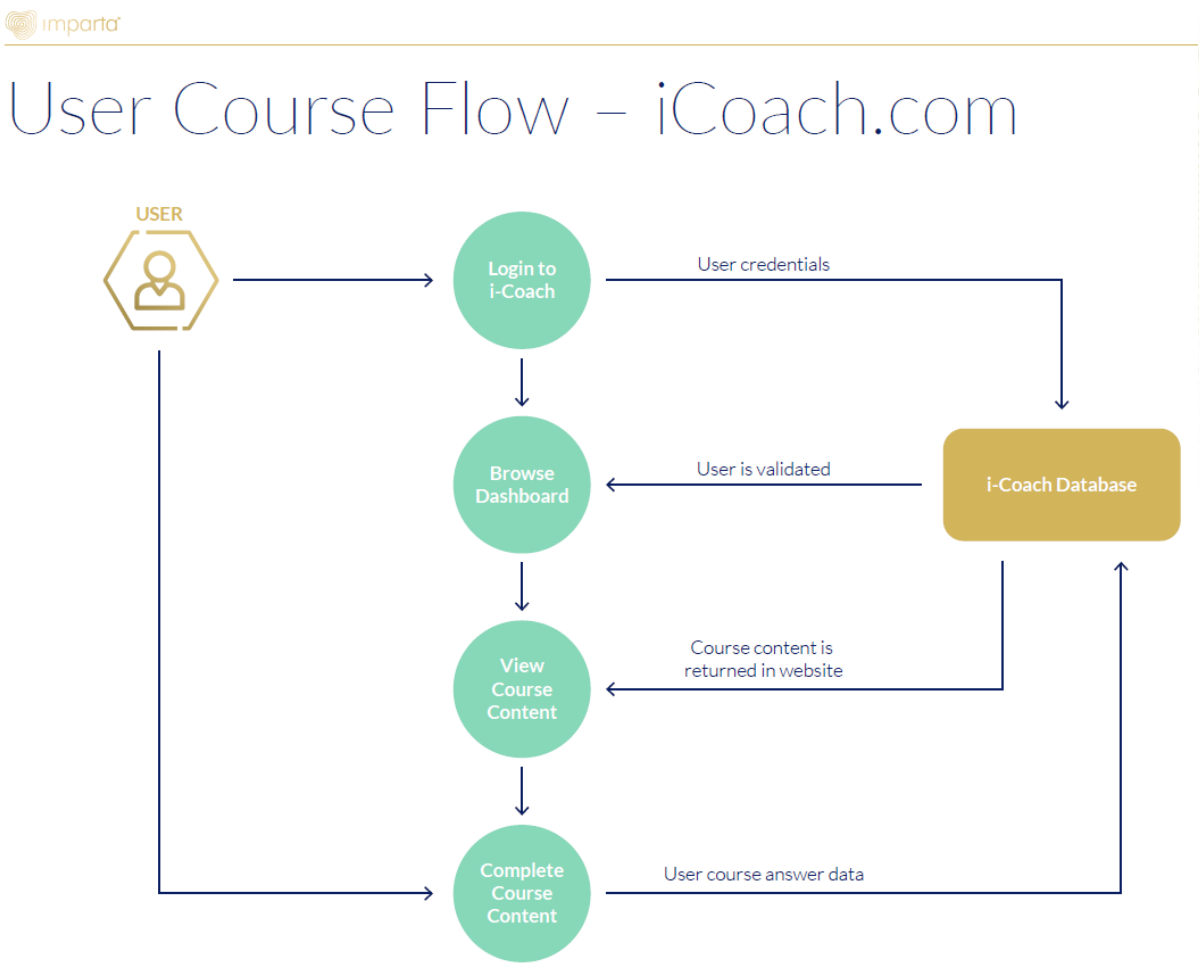
For verification of this certificate, please contact the PQAL UK Office

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

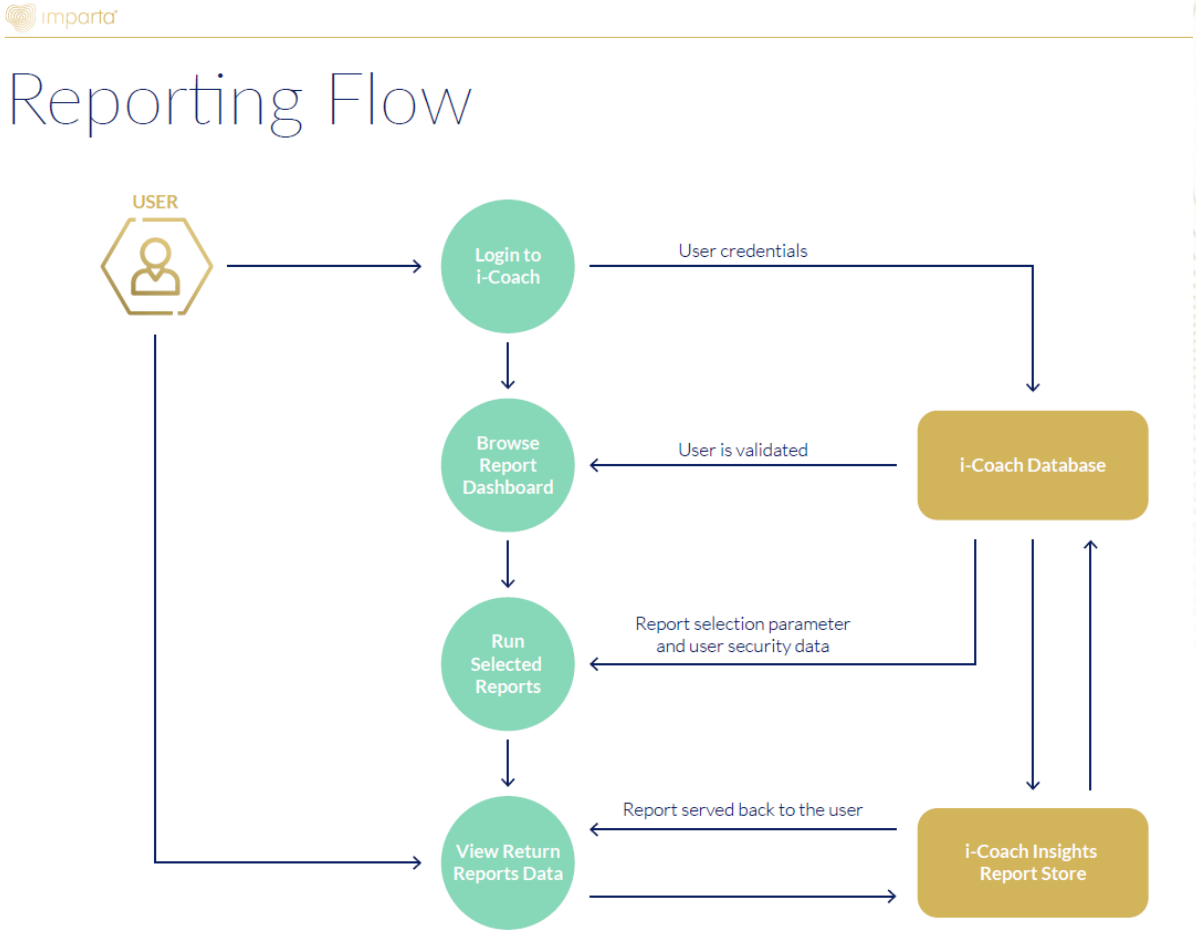
UKAS MANAGEMENT SYSTEMS 9940

Annex B

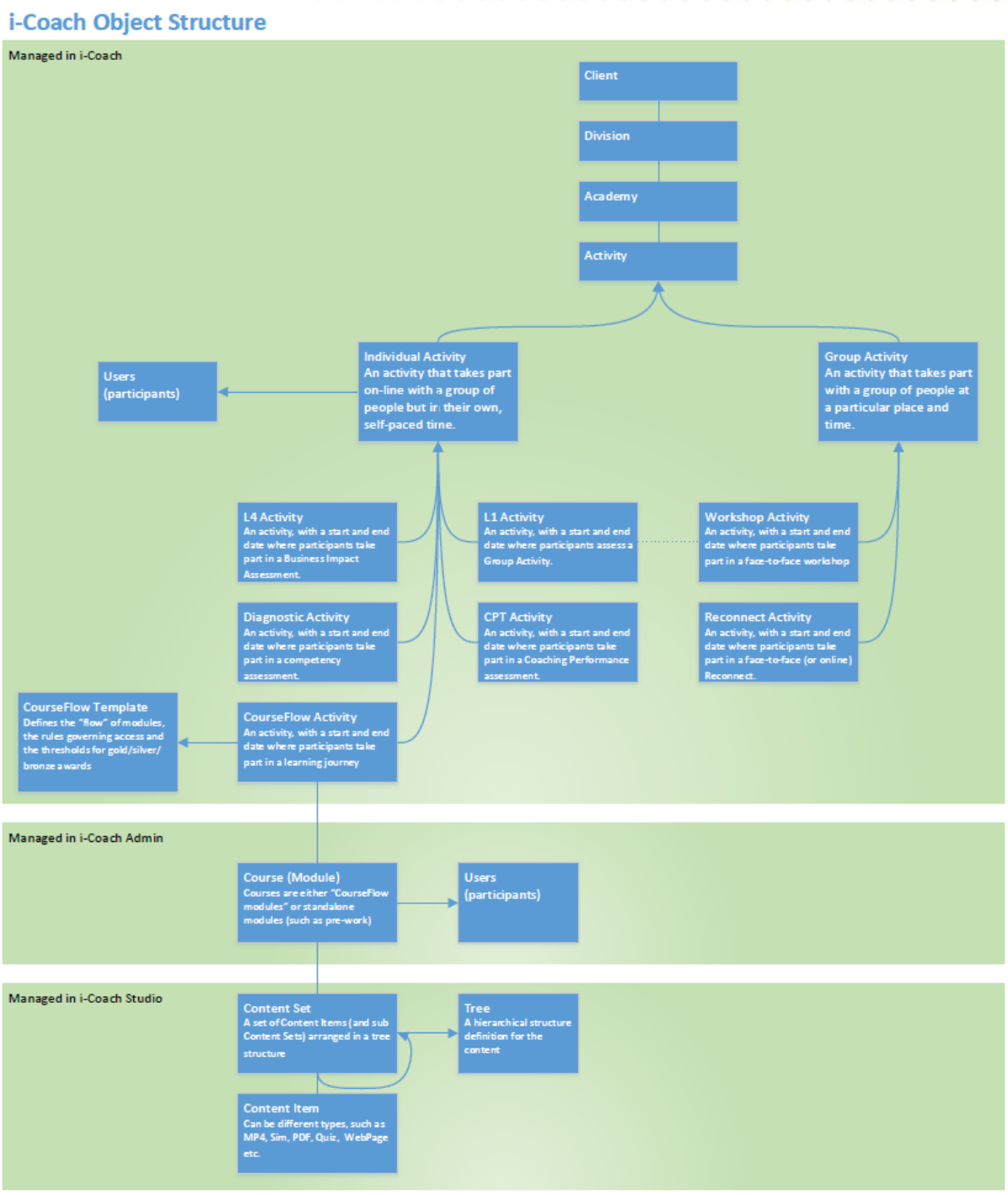
i-Coach User Course Flow diagram



i-Coach Reporting Flow diagram



i-Coach Object Structure



i-Coach Component Architecture