

## ASEC CLIENT PRIVACY PROMISE

ASEC respects its clients' and their associated End Users' privacy and is committed to protecting their Personal Data. This privacy policy informs ASEC's Clients and associated End Users of how ASEC will process their Personal Data.

This privacy policy applies to Personal Data which is Processed by ASEC in providing its Services to Clients and describes ASEC's privacy practices in connection with such Processing.

Depending on the specific Services being used or specific interactions a Client or End User has with ASEC, there may be different or supplemental privacy policies that describe and govern how ASEC use Personal Data. Those different or supplemental privacy policies apply to that specific Service a Client or End User is using or those specific interactions they have with ASEC. Visitors to our website [www.miqyasaldhad.com](http://www.miqyasaldhad.com) should refer to our website privacy notice available there.

Certain defined terms are used in this privacy policy, and for ease of reference, these are set out below:

|                                    |   |
|------------------------------------|---|
| <b>Clients</b>                     | Our clients with whom we have a legal contract for the provision of Services.   |
| <b>Controller</b>                  | The natural or legal person, public authority, agency, or any other body, which alone or jointly with others determines the purposes and means of the Processing of Personal Data.  |
| <b>Educational/School purposes</b> | Services or functions that customarily take place at the direction of the educational institution/agency or their teacher/employee, for which the institutions or agency would otherwise use its own employees, and that aid in the administration or improvement of educational and school activities (e.g., instruction, administration, and development and improvement of products/services intended for educational/school use). |
| <b>End Users</b>                   | Include school administrators, teachers, parents/guardians, and Users. This privacy policy sits alongside any specific privacy notices relating to the use of ASEC's products and/or services and should be read in conjunction with the relevant privacy notice.   |

|                              |  |
|------------------------------|--|
| <b>Personal Data</b>         | Any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).   |
| <b>Process or Processing</b> | Any operation or set of operations that is performed on Personal Data, including collecting, recording, organising, structuring, storing, sharing, viewing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, combining, restricting, erasing, and destroying. |
| <b>Processor</b>             | A natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.   |
| <b>Services</b>              | The products and services provided by ASEC to its Clients and their End Users from time to time, including the ASEC Platform and other online applications and services.   |
| <b>UAE PDPDL</b>             | UAE Federal Decree Law No. 45 of 2021 regarding the Protection of Personal Data.   |
| <b>EUROPEAN GDPR</b>         | European Union's General Data Protection Regulation No. 2016/679.  |

The following principles summarise ASEC's commitment under this privacy policy:

- ASEC only Processes Personal Data for Education/School purposes (including, but not limited to, use relating to instruction, administration, and development and improvement of Services intended for Education/School use)
- ASEC does not use Personal Data for behavioral targeting of advertising.
- ASEC does not sell Personal Data or pass any End User's Personal Data to any unauthorised third parties (see below for details of authorised third parties).
- ASEC follows security best practices to protect Clients and their End Users' Personal Data, including ensuring that the most privacy-friendly options are set by default.
- ASEC reviews Personal Data periodically, updates it when inaccurate, and deletes it when no longer needed.

- ASEC requires a Data Protection Impact Assessment (DPIA) for high risk processing, such as profiling, special data, biometrics, geolocation, or Client's data.
- ASEC adopts the UAE PDPDL.
- ASEC is a proud signatory of the User Privacy Pledge. Details of the User Privacy Pledge can be found **here**.

This privacy policy is provided in a layered format so you can click through to the specific areas set out below:

- Contact details
- Disclaimer
- Changes to the privacy promise
- The data ASEC collect about Clients and their End Users
- If a Client fails to provide Personal Data
- How is the Personal Data collected
- Purposes for which ASEC use Personal Data
- Consent
- Disclosures of Personal Data
- International transfers
- Data security
- Data retention and requests for deletion
- Additional information for certain jurisdictions

#### 1. Contact details

If you have any questions or feedback about this privacy policy, please contact **privacy@miqyasaldhad.com**. End Users of Clients should check with that Client (normally a school or other educational institution) if they have any questions regarding how their Personal Data may be Processed.

#### 2. Disclaimer

SOME LAWS (LIKE THE EUROPEAN GDPR DISTINGUISH BETWEEN A "CONTROLLER" AND A "PROCESSOR" (OR SIMILAR TERMS). WHERE MIQYAS AL DHAD IS PROVIDED PERSONAL DATA IN ITS CAPACITY OF PROVIDING SERVICES TO ITS CLIENTS, THEN MIQYAS AL DHAD WILL ONLY PROCESS THAT PERSONAL DATA IN ACCORDANCE WITH THE INSTRUCTIONS OF ITS CLIENTS AND MIQYAS AL DHAD WILL THEREFORE ACT AS A PROCESSOR IN RESPECT OF SUCH PERSONAL DATA. MIQYAS AL DHAD'S CLIENT WILL BE THE CONTROLLER OF THAT PERSONAL DATA FOR THAT PURPOSE AND WILL BE RESPONSIBLE TO ITS END USERS FOR THE WAY IN WHICH THEIR PERSONAL DATA IS PROCESSED AS THE CONTROLLER. END USERS OF CLIENTS SHOULD THEREFORE CHECK WITH THAT SCHOOL/ORGANIZATION WHO ARE A CLIENT IF THEY HAVE ANY QUESTIONS REGARDING HOW THEIR PERSONAL DATA IS PROCESSED IN COMPLIANCE WITH APPLICABLE LAWS. IN PARTICULAR, CLIENT END USERS WHO SEEK ACCESS TO THEIR PERSONAL DATA, OR WHO SEEK TO CORRECT, AMEND, OR DELETE INACCURATE PERSONAL DATA, SHOULD DIRECT THEIR REQUESTS TO THE SCHOOL/ORGANIZATION WHO ARE MIQYAS AL DHAD'S CLIENTS. CLIENTS MAY BE ABLE TO REMOVE AND UPDATE PERSONAL DATA AND DATA WITHOUT MIQYAS AL DHAD'S INVOLVEMENT.

### 3. Changes to the privacy promise

ASEC keeps its privacy promise under review. This version was last updated on 25 November 2025. ASEC will inform its Clients prior to making any changes to this privacy policy, which ASEC believes will materially impact their rights. As a Client, if you object to any changes, you must notify ASEC within 14 days by email: [privacy@miqyasaldhad.com](mailto:privacy@miqyasaldhad.com). If a Client continues to use the Services after they have received notice of changes to this privacy policy, they will be deemed to have accepted the changes.

### 4. The data ASEC collect about Clients and their End Users

ASEC may process different kinds of Personal Data relating to its Clients and their End Users, which ASEC have grouped together as follows:

**Contact Data:** ASEC takes contact data that includes, but is not limited to, first name, last name, job position, address, phone number, and email address of a Client's account managers, administrators, and any other representatives who ASEC correspond with. Where a Client requires ASEC to contact parents/guardians of User End Users, ASEC will also take contact details, including, but not limited to, first name, last name, address, phone number, and email address of the parents/guardians provided by the Client. The Client is responsible for ensuring the accuracy of the Contact Data that it provides to ASEC.

**End User Account Data:** ASEC creates user accounts to access Services in accordance with a Client's instructions. Where End User accounts are created in accordance with Client instructions, ASEC collects personally identifiable information about them, including, but not limited to, their first names, middle names, surnames, gender, usernames, email addresses, passwords, and the school enrolled on. This information is normally provided by Clients for ASEC to access the Services, but it may be entered by End Users themselves or populated from the End User's account with a third-party sign-in service, such as their Google account.

**Profile Data:** ASEC collects Client and End User's data with respect to their use of the Services. This mainly comprises information relating to the User's enrollment, participation, and progression using the Services, such as school test results (where provided by the Client), diagnostic tests and survey results, performance results from using the Services, and End User interests and preferences when using the Services. This data may also comprise information that is uploaded by the End User (including, but not limited to, their avatar, photos, drawings, files, notes, hyperlinks, and other learning records). ASEC regularly adds types of information that can be uploaded, and these are all considered Profile Data under this privacy policy. If an End User is permitted by the Client to allow ASEC to access the microphone or video recordings on their device, ASEC may also collect video and voice recordings.

**Communications Data:** ASEC collects messages that are sent and received by End Users using the Services, and ASEC also collects any information that a Client or End User sends to ASEC directly through communications, such as emails or phone logs.

**Log Data:** When a Client or End User uses the Services, ASEC receives log data such as their internet protocol (IP) address, log-in data, browser type and version, time zone setting and location, browser plug-in type and version, operating system and platform, device information, and other technology on the devices used to access the Services.

ASEC also collects, uses, and shares aggregated data such as statistical or demographic data for any purpose. Aggregated data could be derived from Personal Data, but is not considered Personal Data as this data will not directly or indirectly reveal an individual's identity. For example, ASEC may aggregate Log Data to calculate the percentage of users accessing a specific feature of the Services, and this aggregated data may be shared with third parties. However, if ASEC combines or connects aggregated data with Personal Data so that it can directly or indirectly identify an individual, ASEC treats the combined data as Personal Data, which will be used in accordance with this privacy policy.

Some laws require heightened data protection measures for special types of Personal Data. For the purposes of this privacy policy, "Special Personal Data" includes details about race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about user health, genetic and biometric data, or information about criminal convictions and offences. Unless otherwise agreed with the Client, ASEC does not knowingly collect any Special Personal Data about Clients or their End Users. ASEC will not be held responsible in circumstances where the Client or End Users provide Special Personal Data. If ASEC discovers that it is Processing Special Personal Data without prior written agreement with the Client, ASEC may take steps to delete such data without any further notice to the Client or End Users.

#### 5. If a Client fails to provide Personal Data

Where ASEC needs to collect Personal Data by law, or under the terms of a contract ASEC has with a Client, and that Client or their End Users fail to provide that data when requested, ASEC may not be able to provide the Client and their End Users with access to the Services.

#### 6. How is the Personal Data collected

ASEC use different methods to collect data from and about Clients and End Users, including:

**Direct interactions.** Clients and their End Users may give ASEC identity and contact details by filling in forms or by corresponding with ASEC by post, phone, email, or otherwise. This includes Personal Data provided when a Client or End User:

- Creates or instructs ASEC to create an End User account.
- Subscribes to ASEC Services or publications.
- Requests support or maintenance services.
- Enters a competition.
- Completes forms.
- Contact ASEC or provide feedback.
- Uploads data onto platforms or applications that form part of the Services, including any direct - communications via such platforms or applications.
- Responds to surveys and questionnaires.

**Automated technologies or interactions.** As Clients and End Users interact with the Services, ASEC will automatically collect Log Data and Profile Data about Clients' and End Users' equipment, actions, and patterns. ASEC may collect this Personal Data by using cookies, cache, and other similar technologies. Clients and End Users are always free to decline cookies if their browser permits, although doing so may interfere with use of the Services.

**Third parties or publicly available sources.** ASEC may receive information about Clients and End Users from Clients themselves and/or from parents/guardians through providing the Services. ASEC may also receive Personal Data about Clients and End Users from various third parties and public sources, including Log Data from analytics providers such as Google.

#### 7. Purposes for which ASEC uses Personal Data

ASEC will only use Personal Data when the law allows it to. Most commonly, ASEC will use Personal Data in the following circumstances:

- Where ASEC needs it to ensure secure End User authentication.
- Where ASEC needs to perform the contract it is about to enter into or has entered into with Clients.
- Where it is necessary for ASEC's legitimate interests (or those of a third party) provided that user interests and fundamental rights are not overridden.
- Where ASEC needs to comply with a legal obligation.

Set out below, in a tabular format, is a description of the ways ASEC uses Personal Data of Clients and End Users who use the Services, and which of the legal bases ASEC relies on to do so.

| Purpose/Activity   | Type of data   | Lawful basis for Processing including basis of legitimate interest  |
|--|--|---|
| To register a new End User.  | (a) End User Account<br>(b) Contact                                      | To deliver the Services in accordance with ASEC's contractual obligations with Clients.   |
| To manage its relationship with its Clients and End Users which will include:<br>(a) Notification about changes to its terms or this privacy policy<br>(b) Asking Clients and End Users to leave a review or feedback, or take a survey. | (a) End User Account<br>(b) Contact<br>(c) Profile<br>(d) Communications | (a) To deliver the Services in accordance with ASEC's contractual obligations with Clients.<br>(b) Necessary to comply with a legal obligation.<br>(c) Necessary for its legitimate interests (to keep records updated and to study how Clients and their End Users use the Services in order to develop the Services and grow its business). |

|  |  |  |
|--|--|--|
| <p>To administer and protect the business and the Services (including fraud detection and violation of ASEC or its Client's terms of use, troubleshooting, data analysis, testing, system maintenance, support, reporting, and</p> | <p>(a) End User Account<br/>(b) Contact<br/>(c) Log<br/>(d) Communications</p>                 | <p>(a) Necessary for legitimate interests (for running its business, provision of administration and IT services, network security, to prevent fraud, and in the context of a business reorganisation or group restructuring exercise).<br/>(b) Necessary to comply with a legal obligation.<br/>(c) To deliver the Services in accordance with ASEC's</p> |
| <p>To provide reports and other information to Clients relating to their End Users and to deliver relevant and personalised education content and platform access to Clients and their End Users, and measure or understand</p>    | <p>(a) End User Account<br/>(b) Contact<br/>(c) Profile<br/>(d) Log<br/>(e) Communications</p> | <p>(a) To deliver the Services in accordance with ASEC's contractual obligations (to notify Clients and End Users about account activity).<br/>(b) Necessary for its legitimate interests (to study how Clients and their End Users use the Services, to develop them and to grow its business).</p>   |
| <p>To use data analytics to improve the Services, customer relationships and experiences.</p>  | <p>(a) Technical<br/>(b) Profile<br/>(c) Communications</p>                                    | <p>Necessary for its legitimate interests (to define types of End Users in order to research, understand, and analyse trends of End Users, which in turn will allow ASEC to keep Services updated and relevant and to grow its business).</p>  |

ASEC will only use Personal Data where such use is compatible with the purposes as outlined above. However, ASEC may Process Personal Data without Clients' or End Users' knowledge or consent, in compliance with the above rules, where this is required by law.

## 8. Consent

As ASEC's Clients are Controllers for Personal Data collected and used as part of the Services, ASEC requires that, where consent is the legal basis for the Processing of any Personal Data or special data, all Clients obtain all necessary consents required under data protection and other laws from End Users before allowing End Users to access the Services. As a Client, you are responsible for checking your local laws to determine the appropriate method of consent and ensuring that consent meets the required standard.

In particular, ASEC does not permit children or minors (as defined by the laws applicable to a Client) to create an account without the consent and at the direction of a parent or, in lieu of parental consent, the School Client. A Client should contact ASEC if it believes ASEC has inadvertently collected information from a child or minor without appropriate consent so that ASEC may delete the information as soon as possible.

## 9. Disclosures of Personal Data

ASEC takes any requests to share Client and End Users' data very seriously, and any approval for data sharing only takes place after an assessment is undertaken on a case-by-case basis. Depending on the Services set up for a Client, ASEC may make User End User data available to teacher and school administrator End Users, as well as registered parents/guardians of User End Users who have Services accounts connected to the User End User (as provided by the Client). Depending on the features and account controls applicable to the Client's accounts, the Services may make User End User Personal Data visible to teachers, school administrators, or parent/guardian End Users (who are linked to the User End User). Further, ASEC may provide access to certain Personal Data to the School for the purpose of monitoring End User usage and activity and evaluating the effectiveness of the Client's use of the Services.

ASEC may share Personal Data for the purposes set out in the table above to third parties to whom ASEC may choose to sell, transfer, or merge parts of ASEC's business or its assets. Those third parties must undergo risk-based due diligence before processing personal data.

Alternatively, ASEC may seek to acquire other businesses or merge with them. If a change happens to ASEC's business, then the new owners may use the Personal Data ASEC has obtained in the same way as set out in this privacy policy.

ASEC may also share Personal Data with its service providers to help enable it to provide its products/services to Clients and End Users.

ASEC requires all third parties to respect the security of Personal Data it shares and to treat it in accordance with the applicable laws and regulations. ASEC does not allow its third party service providers to use Personal Data for their own purposes and only permits them to Process Client and End User Personal Data for specified purposes in accordance with this privacy policy and ASEC's instructions.

ASEC may also disclose Client and End User Personal Data to a third party to comply with applicable laws or regulations, or a valid legal request. If ASEC is going to release Personal Data in this instance, ASEC will use reasonable attempts to provide the relevant Client with notice in advance by email, unless ASEC is prohibited from doing so by law, or otherwise where it is impracticable to do so in the circumstances.

The Services may link to and may be linked by websites operated by other entities or individuals. Some of these websites, such as an ASEC social media page, may be co-branded with the ASEC name or logo. This privacy policy does not apply to, and ASEC cannot always control the activities of, such other third party websites. A Client and/or their End Users should consult the respective privacy policies of those third party websites.

#### 10. International transfers

Unless agreed otherwise in a contract between ASEC and a Client, any Personal Data processed by ASEC pertaining to its Clients or their End Users will be hosted on servers in the UAE, or for Clients situated in Southeast Asia, in Singapore. Notwithstanding the foregoing, during a Client and their End Users use of Services and interactions with ASEC, Personal Data may be transferred outside of a Client's home country and may be stored in and accessed from multiple countries in compliance with applicable laws.

Some of ASEC external third party service providers are also based in jurisdictions outside of those of its Clients and, therefore, the Processing of Personal Data may involve a transfer of data outside of the Client's country. Whenever ASEC transfers Personal Data out of a Client's home country, it ensures a similar degree of protection is afforded to it and ASEC ensures that it follows any data protection laws governing the transfer to and from of Personal Data outside of specific jurisdictions.

#### 11. Data security

ASEC has put in place appropriate security measures to prevent Personal Data from being accidentally lost, used or accessed in an unauthorised way, altered, or disclosed. In addition, ASEC limits access to Personal Data to those employees, agents, contractors, and other third parties who have a business need to know. They will only Process Personal Data on ASEC's instructions, and they are subject to a duty of confidentiality.

To protect Clients' and their End Users' privacy and security, ASEC takes reasonable steps to verify their identity before granting account access or responding to Personal Data requests. For example, ASEC may ask for certain Personal Data to confirm a Client or their End User's identity, and may require that passwords be created and used to access certain parts of its Services. Clients are responsible for ensuring that they and their End Users create and maintain a strong password to help ensure the security of their accounts, and they keep these accounts secure. However, no security measures are perfect, and ASEC cannot ensure or warrant the security of any or all of the information that is shared with ASEC by Clients or their End Users. In the event that any Personal Data is compromised as a result of a breach of security, ASEC will take steps to investigate the situation and will notify the Client of the security incident in accordance with applicable laws and regulations.

## 12. Data retention and requests for deletion

ASEC will delete an End User account when instructed to do so by a Client. ASEC may also delete End User accounts following the termination or expiry of a Client contract. Prior to deleting an account, ASEC will notify the Client associated with the account by email and provide an opportunity to download an archive copy of End User Account Data and Profile Data.

Where ASEC is required to do so by law, ASEC will retain basic information about its Clients after they cease to be Clients. In limited circumstances, ASEC may also retain Client and End User Personal Data for a longer period in the event of a complaint or if ASEC reasonably believes there is a prospect of litigation in respect to ASEC's relationship with a Client.

In some circumstances, ASEC will anonymise Personal Data (so that it can no longer be associated with or identify the Client and/or associated End Users) for analytical purposes, in which case ASEC may use this information indefinitely without further notice.

## 13. Additional information for certain jurisdictions

Additional information about the collection and use of Personal Data relating to prospective and current Clients in certain jurisdictions are set out below under the relevant section.

In certain circumstances, local data protection laws (such as the GDPR and the UAE PDPL) may give Clients and their End Users rights with respect to Personal Data if they are located in or are residents of that country, state, or territory.

### **What rights may be available?**

These rights differ based on local data protection laws in an individual's country, state, or territory, but these rights may include one or more of the following:

- ✓ ask if ASEC holds Personal Data about a Client or their End Users and request copies of such Personal Data and information about how it is Processed (also called an access request);
- ✓ request that inaccurate Personal Data is corrected (also called a rectification request);
- ✓ request deletion of Personal Data that is no longer necessary for the purposes of the Processing, Processed based on withdrawn consent, or Processed in non-compliance with applicable legal requirements (see section 12 of this privacy policy for more information);
- ✓ Request ASEC to restrict the Processing of Personal Data where the Processing is inappropriate or not as anticipated;
- ✓ object to the Processing of Personal Data;
- ✓ request portability of Personal Data that a Client or their End User has provided to ASEC (which does not include information derived from the collected Personal Data), where the Processing of such Personal Data is based on consent or a contract with the Client and is carried out by automated means; and
- ✓ lodge a complaint with the relevant local supervisory authority.

Please consult your local data protection laws to determine what rights may be available to you and which exceptions may apply. If a Client wants to make an access request or a rectification request, the Client can do this themselves using the self-service functionality via applications or platforms that provide the Services. If, for any reason, a Client is unable to access the data or make any changes via the self-service functionality, the Client can contact ASEC via the helpdesk using the following email address: **info@miqyasaldhad.com**

For all other rights under applicable law, a Client can exercise its rights on behalf of itself or its End Users by contacting ASEC by email at **privacy@miqyasaldhad.com**. ASEC endeavour to comply with these requests within one calendar month of your request; however, in certain circumstances, it may take longer if your request is complex or excessive. If this is the case, ASEC will let you know. End Users of Clients should contact the Client if they want to exercise their rights under applicable law.