Data Protection Policy

Contents

1. Overview

1.1 Policy introduction

English Speaking Board (International) Ltd. is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, trustees, contractors, centres, learners, clients, members, suppliers andother individuals for a variety of business purposes.

1.2 Purpose

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that their manager and through them the senior management team is consulted before any significant new data processing activity is initiated to ensure that relevant compliancesteps are addressed.

1.3 Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amendthis policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

1.4 Communication

This policy will be approved by the Board of Trustees during their quarterly meeting and communicated to all staff during the monthly staff meeting.

1.5 Policy review

ESB International will review this policy at least annually, to ensure its procedures and practices continue to meet legislative and regulatory compliance. If required, ESB International reserves the right to make changes at any time in line with customer and stakeholder feedback, changes in its practices as a result of actions from the regulatory authorities, external agencies, or in compliance with changes in government legislation.

Responsible Officer

The Chief Executive has overall responsibility for the day-to-day implementation of this policy. You shouldcontact the Chief Executive for further information about this policy if necessary.

1.6 Principles

English Speaking Board (International) Ltd. shall comply with the principles of data protection (the Principles)enumerated in the UK General Data Protection Regulation (UK GDPR). We will make every effort possible in everything we do to comply with these principles.

The Principles are:

1. Lawful, fair and transparent
Data collection must be fair, for a legal purpose and we must be open and transparent as to how thedata will be used.

2. Limited for its purpose
Data can only be collected for a specific purpose.

3. Data minimisation
Any data collected must be necessary and not excessive for its purpose.

4. Accurate
The data we hold must be accurate and kept up to date.

5. Retention
We cannot store data longer than necessary.

6. Integrity and confidentiality
The data we hold must be kept safe and secure.

1.7 Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. As an employee, you are responsible for keeping a written record of how all the data processing activities you carry out comply with each of the Principles. This record must be kept up to date and must be approved by the Senior Leadership Team.

To comply with data protection laws and the accountability and transparency Principle of UK GDPR, we must demonstrate compliance. As an employee, you are responsible for understanding your particular responsibilities to ensure wemeet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Implement measures to ensure privacy by design and default, including:o Data minimisation
  - o Transparency
  - o Allowing individuals to monitor processing
  - o Creating and improving security and enhanced privacy procedures on an ongoing basis

2. Procedures

2.1 Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose detailswe are processing has consented to this happening.

If we cannot apply a lawful basis (explained in 2.3 below), our processing does not conform to the first principleand will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

2.2 Controlling vs. processing data

English Speaking Board (International) Ltd. is classified as a data controller. We mustmaintain our appropriate registration with the Information Commissioners Office (ICO) in order to continue

lawfully controlling and processing data.

For the purpose of learners data we, and the centre the learners belong to, are joint controllers and must therefore comply with our contractual obligations.

Our responsibilities as a joint data controller:

- **Obligations of controllers**: We need to decide with our fellow joint controllers who will carry out which controller obligation under the UK GDPR. However, regardless of those arrangements, each controller remains responsible for complying with all the obligations of controllers under the UK GDPR.
- **Transparent arrangement**: We must have a transparent arrangement that sets out our agreed roles and responsibilities for complying with the UK GDPR. The main points of this arrangement should be made available to individuals.
- **Individuals' rights**: In particular, we must decide (and be transparent about) how we will comply with transparency obligations and individuals' rights.

If you are in any doubt about how we handle data, contact the Chief Executive for clarification.

2.3 Lawful basis for processing data

We must establish a lawful basis for processing data. As an employee, you must ensure that any data you are responsible for managing has a written lawful basis approved by the Chief Executive. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. Consent
We hold recent, clear, explicit, and defined consent for the individual's data to be processed for aspecific purpose.

2. Contract
The processing is necessary to fulfil or prepare a contract for the individual.

3. Legal obligation
We have a legal obligation to process the data (excluding a contract).

4. Vital interests
Processing the data is necessary to protect a person's life or in a medical situation.

5. Public function
Processing is necessary to carry out a public function, a task of public interest or the function has a clearbasis in law.

6. Legitimate interest
The processing is necessary for our legitimate interests. This condition does not apply if there is a goodreason to protect the individual's personal data, which overrides the legitimate interest.

3. Special categories of personal data

Previously known as sensitive personal data, this refers to data about an individual which is more

sensitive, therefore requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion/philosophical beliefs
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's explicitconsent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not havea lawful basis for processing special categories of data that processing activity must cease.

4. Responsibilities

4.1 Our responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal databreaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data becompromised

4.2 Your responsibilities as an employee

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and arejustified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach dataprotection laws and our policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious orcontradictory to this policy or our legal obligations without delay

4.3 Responsibilities of the Chief Executive of English Speaking Board (International) Ltd.

- Keeping the board updated about data protection responsibilities, risks and issues
- Approving all data protection procedures and policies on a regular basis

- Arranging data protection training and advice for all staff members and those included in thispolicy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is beingheld on them by us
- Checking and approving with third parties that handle the company's data any contracts oragreement regarding data processing

4.4 Responsibilities of the IT Lead reporting to the Chief Executive

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioningproperly
- Researching third-party services, such as cloud services the company is considering using tostore or process data

4.5 Responsibilities of the Quality Assurance Manager

- Reviewing all data protection procedures and policies on a regular basis
- Reviewing data protection queries from centres and/or learners and ensuring their individuals' rights are exercised accordingly

4.6 Responsibilities of the Business Strategy Optimisation Coordinator

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the Chief Executive to ensure all marketing initiatives adhere to the UK data protection law and the company's Data Protection Policy

4.7 Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for anyunconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that informationis inaccurate you should record the fact that the accuracy of the information is disputed and inform your Manager, who will then liaise with the Quality Assurance Team to review the data in question.

5. Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal dataas a service on our behalf, the Chief Executive will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

5.1 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place

whereunauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. Weencourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked awaysecurely when they are not being used
- The Chief Executive must approve any 'cloud' used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

5.2 Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but shouldbe determined in a manner consistent with our data retention schedule.

5.3 Transferring data internationally

The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations. These restrictions apply to all transfers, no matter the size of transfer or how often they are carried out. A transfer of personal data to a separate organisation located outside of the UK is referred to as a restricted transfer. Restricted transfers from the UK to other countries, including to the EEA, are subject to transfer rules under the UK regime. These UK transfer rules broadly mirror the EU GDPR rules, but the UK has the independence to keep the framework under review.

'Adequacy' is a term that the EU uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU.
An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU does. On 28 June 2021, the EU Commission published its adequacy decisions in respect of the UK.
These decisions contain the European Commission's detailed assessment of the UK's laws and systems for protecting personal data, as well as the legislation designating the UK as adequate. These adequacy decisions are expected to last until 27 June 2025. The European Commission will decide whether to extend the adequacy decisions for the UK for a further period up to a maximum of another four years. If they don't extend the decisions, then they will expire on 27 June 2025.

The UK government has also got the power to make its own 'adequacy decisions' in relation to third countries and international organisations.

If there are no UK adequacy regulations about the country, territory or sector for the restricted transfer, the transfer must be subject to appropriate safeguards. Transfer of data for our standard day to day procedures is based on ESB International contracts with registered centres and contractors.

You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the Chief Executive.

6. Rights of individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. Wemust ensure individuals can exercise their rights in the following ways:

1. **Right to be informed**
   - Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
   - Keeping a record of how we use personal data to demonstrate compliance with the needfor accountability and transparency.
2. **Right of access**
   - Enabling individuals to access their personal data and supplementary information
   - Allowing individuals to be aware of and verify the lawfulness of the processing activities
3. **Right to rectification**
   - We must rectify or amend the personal data of the individual if requested because it isinaccurate or incomplete.
   - This must be done without delay, and no later than one month. This can be extended totwo months with permission from the Chief Executive.
4. **Right to erasure**
   - We must delete or remove an individual's data if requested and there is no compellingreason for its continued storage and/or processing.
5. **Right to restrict processing**
   - We must comply with any request to restrict, block, or otherwise suppress the processingof personal data.
   - We are permitted to store personal data if it has been restricted, but not process it further.We must retain enough data to ensure the right to restriction is respected in the future.
6. **Right to data portability**
   - We must provide individuals with their data so that they can reuse it for their ownpurposes or across different services.
   - We must provide it in a commonly used, machine-readable format, and send it directly toanother controller if requested.
7. **Right to object**
   - We must respect the right of an individual to object to data processing based on legitimateinterest or the performance of a public interest task.
   - We must respect the right of an individual to object to direct marketing, including profiling.
   - We must respect the right of an individual to object to processing their data for scientificand historical research and statistics.

8. **Rights in relation to automated decision making and profiling**
   - We must respect the rights of individuals in relation to automated decision making andprofiling.
   - Individuals retain their right to object to such automated processing, have the rationaleexplained to them, and request human intervention.

7. Privacy notice

A privacy notice must be supplied at the time the data is obtained, if obtained directly from the data

subject.If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, i.e. within one month. If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest, when the firstcommunication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the databeing disclosed.

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free ofcharge and must be written in clear and plain language, particularly if aimed at children.

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period,including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only fordata not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about howthose decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement orobligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

8. Subject Access Requests

An individual has the right to receive confirmation that their data is being processed, access to their personaldata and supplementary information which means the information which should be provided in a privacy notice.

8.1 Process for subject access requests

We must provide an individual with a copy of the information they request, free of charge. This must occurwithout delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but theindividual must be informed within one month. You must obtain approval from the Chief Executive before extending the deadline.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the

individual specify the information they are requesting. This can only be done with express permission fromthe Chief Executive.

Once a subject access request has been made, you must not change or amend any of the data that has beenrequested. Doing so is a criminal offence.

8.2 Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to theindividual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the Chief Executive first.

9. Right to erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originallycollected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest forcontinuing the processing
- Where the individual objected to the use of their data for direct marketing purposes
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child for an online service

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of officialauthority
- To comply with a legal obligation such as financial or other regulation
- For archiving purposes in the public interest, scientific research, historical research or statisticalpurposes
- The exercise or defence of legal claims
- For special category data - for public health purposes in the public interest

If the above exemptions apply, we can either fully or partially refuse to comply with your request.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them ofthose recipients.

10. The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation.We must cease processing unless:

- The processing is required to comply with a legal obligation such as financial or other regulation.
- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in theprivacy notice. We must offer a way for individuals to object online.

11. Third parties

11.1 Joint controllers and third party data processors

As a data controller, we must have written contracts in place with any joint data controllers or third party data processors that we use. The contract must contain specific clauses which set out our andtheir liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPRand that the rights of data subjects will be respected and protected.

We acknowledge ourresponsibilities as a data controller under GDPR and we will protect and respect the rights of data subjects.

11.2 Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses.
Our contracts with data processors must set out the subject matterand duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller as well as the processor.
At a minimum, our contracts with processors must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a writtencontract
- The controller will assist the processor in dealing with subject access requests and allowing datasubjects to exercise their rights under UK GDPR
- The processor will assist the controller in meeting its UK GDPR obligations in relation to the securityof processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for thecontroller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on UK GDPR.

Our contracts with joint data controllers must clearly state that both parties are controllers of the data and are both responsible for compliance with the controller obligations under the UK data protection law. They must also specify which controller has the primary responsibility for complying in particular with transparency obligations and individuals' rights.

12. Criminal offence data

Any criminal record checks require lawful basis for processing. Criminal record checks cannot be undertaken based solely onthe consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal convictions and offences or related security measures is considered as a separate set of personal data and referred to as 'criminal offence data'It can only be processes if the processor is either:

- Under the control of official authority; or
- Authorised by domestic law

As a charity organisation, ESB International is under the control of official authority and therefore has the requirement to process certain criminal offence data.

13. Audits, monitoring and training

13.1 Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the Chief Executive and normal procedures.

13.2 Monitoring

Everyone must observe this policy. The Chief Executive has overall responsibility for this policy. You must notify theChief Executive of any breaches of this policy. You must comply with this policy fully and at all times.

13.3 Training

You will receive adequate training on provisions of UK data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities and require further training, you are responsible for requestingnew data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact your line manager.

14. Reporting breaches

Any breach of this policy or of UK data protection law must be reported as soon as practically possible. This means as soon as you have become aware of a breach.

ESB International has a legal obligation to report data breaches to ICO and Ofqual as per their respective requirements.

A personal data breach means a breach of security leading to:

- destruction,
- loss,

- alteration,
- unauthorised disclosure of,
- unauthorised access to personal data
- accessibility
- inaccuracies

A personal data breach is not limited to technology, it can be a verbal breach, hard copy breach as well as in emails or IT systems

All members of staff have an obligation to report actual or potential data breaches. This allows us to:

- Investigate the data breach and take remedial steps if necessary
- Maintain a register of data breaches
- Notify ICO or Ofqual of data breaches that are material either in their own right or as part of a pattern if required

Data breaches or possible data breaches must be reported as soon as possible to your Manager who will liaise with the QA Team and CEO to ensure it is dealt with appropriately. Any member of staff who fails to notify their manager of a data breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures, will be liable to disciplinary action.

15 Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation atrisk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinaryaction under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact your line manager or the Chief Executive.

Revision No	Change to previous release
2	1.2 policy purpose distinguished 1.5 policy review information added updated to replace the EEA with the UK and added reference to third parties based outside the UK 2.2 joint controllers responsibilities added Point 3 – special categories of personal data – updated 4.5 responsibilities of the QA Manager added 4.6 role title updated 4.7 internal process for reporting of data inaccuracy updated Point 5 – DPO information removed as we are not required to have one 5.3 information about international transfers requirements added Point 9 updated to cover rejection of data erasure in order to comply with legal and regulatory obligation and requirements to erase data processed for marketing purposes Point 10 updated to cover compliance with legal and regulatory obligation Point 11 updated to clarify our third party obligations Point 12 criminal offence data details provided Point 14 – definition of data breaches added, process details updated