Data Protection Policy

Contents

1. Overview

1.1 Policy introduction

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

ESB International holds personal data about their employees, trustees, patrons, contractors, centres, satellite centres, venues, learners, clients, members, suppliers and other individuals for a variety of business purposes.

1.2 Purpose

This policy sets out how ESB International seeks to protect personal data and ensure that its staff and contractors who handle personal data understand the rules governing their use of the personal data to which they have access to in the course of their work. In particular,this policy requires them to ensure that their line manager and through them the senior leadership team (SLT) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.3 Scope

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

This policy supplements ESB International's other policies relating to internet and email use. ESB International may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff and contractors 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. All contractors who handle personal data will be informed of the changes to this policy via email notification.

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 should contact the Chief Executive for further information about this policy if necessary.

2. ESB International adherence to Data Protection 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). ESB International will make every effort possible to comply with these principles.

The Principles are:

2.1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and ESB International must be open and transparent as to how the data will be used.

ESB International must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that ESB International should not process personal data unless the individual whose details are being processed has consented to this happening. ESB International must establish a lawful basis for processing all personal data collected.

All personal data collected by ESB International is processed on the contractual basis, where the processing is necessary to fulfil or prepare a contract for data subject and/or their contracting organisation or on the basis of legitimate interest. On rare occasions, when ESB International has to process special category personal data, it is always processed on the base of explicit consent.

If ESB International cannot apply a lawful basis, the processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

2.2. Limited for its purpose

Data can only be collected for a specific purpose.

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

All personal data collected by ESB International is collected for a specific purpose clearly identified within contract documentation with data subject and/or their contracting organisation.

2.3. Data minimisation

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

ESB International regularly reviews all its data collection methods to ensure that collected data continues to be adequate, relevant and not excessive.

2.4. Accurate

The data ESB International holds must be accurate and kept up to date.

All ESB International staff are trained in how to collect accurate data and how to maintain it. It is also the responsibility of the data subject (or, in case of the learners, the centre that provided us with their learners' personal data) to ensure that data held by ESB International is accurate and up to date.

All ESB International application documentation will include a statement that the data contained is accurate at the date of submission.

Employees, contractors, centres and any other third parties are required to notify ESB International of any changes in circumstances to enable personal records to be updated accordingly. It is then the responsibility of ESB International to ensure that any notification regarding change of circumstances is recorded and acted upon.

2.5. Retention

ESB International cannot store data longer than necessary.

ESB International retains personal data for as long as is necessary, at which point it will be securely deleted or destroyed. What is considered necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained. This decision will be determined in a manner that is consistent with ESB International's data retention schedule. Due to the nature of the organisation, ESB International must keep certain learners' data permanently in order to be able to confirm the validity of certificates issued.

All personal data collected by ESB International is subject to retention periods specified within the schedule, which is monitored by the QA Manager and shared with SLT members on a regular basis.

2.6. Integrity and confidentiality

The data ESB International holds must be kept safe and secure.

ESB International has appropriate technical and organisational measures in place in order to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
ESB International must keep personal data secure against loss or misuse.

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised 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. ESB International encourages all staff and contractors who handle personal data 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 away securely when they are not being used
- The Chief Executive must approve any 'cloud' used to store personal 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

Where other organisations process personal data as a service on ESB International's 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.

2.7. Accountability and transparency

ESB International must ensure accountability and transparency in all use of personal data. ESB International must show how it complies with each Principle. In creating this policy, ESB International has set out how it

complies with the Principles. Standard Operating Procedures (SOPs) are in place for all activities related to the handling of personal data, which all staff (employees and contractors) must follow.

To comply with data protection laws and the accountability and transparency Principle of UK GDPR, ESB International must demonstrate compliance. All ESB International's employees and contractors handling personal data provided by ESB International are responsible for understanding their particular responsibilities to ensure ESB International meets 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:
    - Data minimisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

3. Controlling vs. processing data

ESB International is classified as a data controller. ESB International must maintain their appropriate registration with the Information Commissioners Office (ICO) in order to continue lawfully controlling and processing data.

As a data controller, ESB International must have written contracts in place with any joint data controllers or third party data processors used. The contract must contain specific clauses which set out ESB International's and their liabilities, obligations and responsibilities. ESB International must only appoint processors who can provide sufficient guarantees under UK GDPR and that the rights of data subjects will be respected and protected. ESB International acknowledges the responsibilities as a data controller under UK GDPR and will protect and respect the rights of data subjects.

3.1 Joint Controllers

For the purpose of learners' data ESB International and the centre the learners belong to, are joint controllers and must therefore comply with their contractual obligations.

ESB International's responsibilities as a joint data controller:

- **Obligations of controllers**: ESB International need to decide with their 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**: ESB International must have a transparent arrangement that sets out the 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, ESB International must decide (and be transparent about) how to comply with transparency obligations and individuals' rights.

ESB International's 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.

These responsibilities are clarified and agreed by ESB International and all their centres within individual centre agreements and/or contracts signed before any personal learner data is exchanged between ESB International and its centre.

3.2 Third Parties

ESB International's contracts with data processors must set out the subject matter and the duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and ESB International's obligations and rights as the controller as well as the obligations and rights of the third party as a processor.

At a minimum, ESB International's contracts with processors 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 written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under UK GDPR
- The processor will assist the controller in meeting its UK GDPR obligations in relation to the security of 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 the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on UK GDPR

All ESB International agreements and contracts comply with the standards set out by the ICO and take into consideration additional risks associated with organisations established in countries where data protection regime is different than the UK one.

4. 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

From all special categories listed above, ESB International only collects individuals' health data. This is collected in relation to:

1. the learners' application for reasonable adjustments and/or special considerations. In these cases, ESB International will require the data subject's explicit consent to collect this type of special category data. Any such consent will clearly identify the relevant special category data, why it is being processed and to whom it will be disclosed.
2. employees, when ESB International is required to do this by law e.g. to comply with legal obligations to ensure health and safety at work.

It is only in exceptional circumstances that ESB International would collect any other special category of personal data and it would always be preceded by establishing a relevant lawful basis for processing.

5. 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 processed if the processor is either:

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

Any criminal record checks (CRB checks) require lawful basis for processing and cannot be undertaken based solely on the consent of the subject. ESB International grounds for carrying out CRB checks are listed below:

- As an organisation working with the children and vulnerable adults, ESB International requires all of their staff and contractors working directly with these groups, to complete a standard DBS check beforehand.
- As a charitable organisation under the control of the official authority, ESB International is also required to ensure all of the Trustees and Senior Managers are not subject to an automatic disqualification.

ESB International cannot keep a comprehensive register of criminal offence data and only keeps a reference number of all DBS checks completed.

6. Responsibilities

a. ESB International's responsibilities

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

b. ESB International's employees and/or contractor responsibilities for handling personal data

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with ESB International's 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 data protection laws and ESB International's policies through your actions

- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or ESB International's legal obligations without delay
- If you believe that any personal information ESB International holds is inaccurate, record the fact that the accuracy of the information is disputed and inform your Manager

c. Responsibilities of the Chief Executive of ESB International

- 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 this policy
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

d. 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 functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process personal data

e. 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
- Providing advice to the CEO and responding to questions on data protection from staff, board members and other stakeholders
- 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

If in doubt about how ESB International handles personal data, the Quality Assurance Manager should be contacted for clarification.

7. 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 has adequacy regulations about the following countries and territories*:

- The European Economic Area (EEA) countries (these are the EU member states and the EFTA States)

  The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

  The EFTA states are Iceland, Norway and Liechtenstein.

- EU or EEA institutions, bodies, offices or agencies;
- Gibraltar;
- The Republic of Korea; and
- Countries, territories and sectors covered by the European Commission's adequacy decisions (in force at 31 December 2020)

  These include a full finding of adequacy about the following countries and territories:
  Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

  In addition, the partial findings of adequacy about:
  - Japan – only covers private sector organisations
  - Canada – only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)

* Information based on ICO guidance correct at the time of this policy being issued

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 ESB International's standard day-to-day procedures is based on ESB International contracts with registered centres and contractors.

ESB International's agreements with its centres take into consideration the location of the centre and, if required, contain additional ESB International Data Transfer Agreement (IDTA) to ensure compliance with international transfers regulations.

Employees of ESB International must not transfer personal data outside of ESB standard operating procedures, without express permission from the Chief Executive.

8. Rights of individuals

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

i. 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 ESB International uses personal data to demonstrate compliance with the need for accountability and transparency

ii. 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

iii. Right to rectification

- ESB International must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the Chief Executive.

iv. Right to erasure

- ESB International must delete or remove an individual's data if requested and there is no compelling reason for its continued storage and/or processing

v. Right to restrict processing

- ESB International must comply with any request to restrict, block, or otherwise suppress the processingof personal data
- ESB International is permitted to store personal data if it has been restricted, but not process it further.ESB International must retain enough data to ensure the right to restriction is respected in the future.

vi. Right to data portability

- ESB International must provide individuals with their data so that they can reuse it for their own purposes or across different services
- ESB International must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested

vii. Right to object

- ESB International must respect the right of an individual to object to direct marketing, including profiling
- ESB International must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task
- ESB International must respect the right of an individual to object to processing their data for scientific and historical research and statistics

viii. Rights in relation to automated decision making and profiling

- ESB International must respect the rights of individuals in relation to automated decision making and profiling
- Individuals retain their right to object to such automated processing, have the rationaleexplained to them, and request human intervention

9. Privacy notice

ESB International's Privacy Policy is reviewed on an annual basis and available on ESB International's website.

All individuals, for whom ESB International holds personal data and obtains it directly from the data subject (employees, trustees, patrons, contractors, centres, clients, members, suppliers etc.), are requested within their contract to familiarise themselves with ESB International's Privacy Policy and provided with a link to ESB International's website.

All individuals, for whom ESB International holds personal data but does not obtain it directly from the data subject (satellite centres, venues, learners etc.) are provided with a link to ESB International's Privacy Policy by their centre. The centre must inform their learners how their personal data will be used and about their rights as data subjects as per the centre agreement issued by ESB International.

10. Subject access requests

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

a. Process for subject access requests

ESB International must provide an individual with a copy of the information they request, free of charge. This must occur without delay, and within one month of receipt. ESB International 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 the individual must be informed within one month. ESB International's employee must obtain approval from the Chief Executive before extending the deadline.

ESB International 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, ESB International can request the individual specify the information they are requesting. This can only be done with express permission from the Chief Executive.

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

b. Data portability requests

ESB International 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. ESB International must provide this data either to the individual 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 an ESB International' employee making the extension must receive express permission from the Chief Executive first.

11. The right to erasure

As an awarding organisation ESB International has an obligation to retain information on all learners' certificates issued and therefore ESB International is unable to erase their learners' data from the systems.

For data relating to any other individuals, in certain circumstances, they have a right to have their data erased and for processing to cease:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing 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

ESB International 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 official authority
- To comply with a legal obligation such as financial or other regulation
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims
- For special category data - for public health purposes in the public interest

If the above exemptions apply, ESB International can either fully or partially refuse to comply with data subject's 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, ESB International must inform them ofthose recipients.

12. The right to object

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

- The processing is required to comply with a legal obligation such as financial or other regulation
- ESB International has 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

ESB International must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. ESB International's Privacy Policy explains how data subjects can exercise this right.

13. Audits, monitoring and training

a. 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. ESB International's employees and contractors who handle personal data provided by ESB International must conduct a regular data audit as defined by the Quality Assurance Manager and normal procedures.

b. Monitoring

ESB International's employees and contractors who handle personal data provided by ESB International must observe this policy and comply with it fully and at all times.

The Chief Executive has overall responsibility for this policy. Any breaches of this policy must be raised with the Chief Executive immediately.

c. Training

ESB International's employees and contractors who handle personal data provided by ESB International will receive adequate training on provisions of UK data protection law specific for their role. All training must be completed as requested. If an employee moves role or responsibilities and requires further training, new data protection training relevant to the new role or responsibilities will be provided if needed.

Employees who require additional training on data protection matters, should contact their line manager.

14. Reporting breaches

Any breach of this policy or of the 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 its regulators (Ofqual, Qualifications Wales and CCEA) 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 employees and contractors who handle personal data have an obligation to report actual or potential data breaches. This allows ESB International to:

- Investigate the data breach and take remedial steps if necessary
- Maintain a register of data breaches
- If required, notify ICO and/ or its regulators of data breaches that are material either in their own right or as part of a pattern

Data breaches or possible data breaches identified by an employee must be reported as soon as possible to the line manager who will liaise with the QA Team and CEO to ensure the issue is dealt with appropriately. Any employee who fails to notify their line 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

ESB International takes compliance with this policy very seriously. Failure to comply puts both employees/contractors and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under ESB International's procedures which may result in dismissal. If employees/contractors have any questions or concerns about anything in this policy, they must contact their line manager, Quality Assurance 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
3	Section 1.3 updated with additional groups - patrons, satellite centres and venues Section 4 – responsibilities of the Business Strategy Optimisation Coordinator removed and allocated to QA Manager All contents restructured to improve clarity and generic requirements information replaced with specific procedures applied by ESB International