ASSOCIATION OF RUSSIAN BALLET & THEATRE ARTS

(non-profit making organisation)

Patrons: Mikhail Messerer, Olga Sebadoch, Svetlana Adyrkhaeva, Elena Glurjidze

ARBTA DATA PROTECTION POLICY

The Context

ARBTA needs to retain and process essential data in order to enable it to operate successfully. This includes certain personal data related to our employees, customers, candidates and others associated with the organisation. ARBTA is the data 'controller'.

ARBTA is required to record, keep, maintain, process and retain necessary personal data for the purposes of processing its 'examinations' operations within its legal obligations.

The data managed is about candidates, teachers, examiners/assessors, officers/HQ staff, directors and that of associated 'centres' and organisations. These are each referred to as 'data subjects'.

Data Processing Principles

The Data Protection Act lists eight principles which detail the legal conditions that must be adhered to by ARBTA when obtaining, handling, moving and storing personal data. Information must:

- *Be fairly and lawfully processed and that the information shall not be processed or used unless certain conditions are met.*
- *Be processed for limited purposes and in a specified manner compatible with that purpose;*
- *be adequate, relevant and not excessive for those purposes; and only to the extent that it is needed to fulfill operational needs or to comply with any legal requirements.*
- *Be accurate, and where necessary, kept up to date.*
- *Not to be kept for longer than is necessary for that purpose.*
- *Be processed in accordance with the data subject's rights, and ensuring that the rights of people about whom information is held can be exercised fully under the Act. These include: (i) the right to be informed that processing is being undertaken, (ii) the right of access to one's personal information; (iii) the right to prevent processing in certain circumstances; (iv) the right to correct, rectify, block or erase incorrect information.*
- *Be kept safe and secure from unauthorised access, unlawful processing, accidental loss of destruction or damage by using appropriate technical and organisational measures.*
- *Not to be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.*

Employee Obligations

All employees are required to take practical steps to comply with the principles, ensuring personal data is never left visible or unattended on a desk, photocopier or computer screen. Personal data must not be left on the desk when not at work.

During the course of your work you are likely to have access to information which is private or confidential to ARBTA. You have a responsibility for the preservation of the confidentiality and integrity of information used during the course of your work.

Staff should consider the following list before recording personal data:

- Is this information needed?
- Is this information 'ordinary' or 'sensitive'?
- Does ARBTA have the 'data subjects' consent?
- Are you authorised to deal with this data?
- Has the data come from a secure source or do you need to check with the data subject it is accurate?

- Is the data recorded secure?

Compliance is your professional responsibility, failure to follow the above obligations or comply with the Data Protection principles may be considered a disciplinary matter.

Data Security

ARBTA will:

- Prevent unauthorised access to personal data including electronic and paper based forms.
- Ensure the storage of personal data in any form is secure.
- Ensure computer systems are reliable, virus protected and secure.
- Ensure computer systems and servers are password protected.
- Ensure only authorised staff are given passwords.
- Prevent computer screens being overlooked by unauthorised people.
- Ensure all staff who manage data are trained to comply with the Data Protection Acts.
- Have in place methods for identifying date security breaches, investigating them and preventing them.
- Have secure procedures for backing up data.
- Have a secure method for the disposal of unwanted storage devices and printouts.
- Not allow staff without permission to (i) develop new computer systems to process data, (ii) process data for a new purpose, (iii) create new manual filing systems, or (iv) manually file for a new purpose.

Data Processing Consent

ARBTA will inform all its data subjects its need to process 'ordinary' data for its examination processing purposes. In the case of 'sensitive' data individual consent to process the data will be obtained.

Data Subject Obligations

Defined for the purposes of this ARBTA's context as an Awarding Organisation as the candidates' or learners' obligations.

Candidates, or if under 16 their parents/guardians, will be advised by the person who registers them i.e. their 'centre' teacher about the information that ARBTA will collect, use and retain about them, and to whom the information will be shared with. Candidates must ensure their personal information is correct and up to date, they must ensure that any changes are notified to ARBTA, who cannot be held responsible for subsequent errors. ARBTA will not share personal information in any form to unauthorised third parties.

Data Subject Access

Individuals whom ARBTA holds personal data are entitled to:

- ask what information is held by ARBTA and why;
- ask how they can access it;
- be informed how they can update it;
- be informed how ARBTA complies with the 1998 Data Protection Act.

The Data Protection Act (1998) and the Freedom of Information Act (2000) provides an individual with the right to access their personal information held by ARBTA, including electronically held data (and emails), and systemised filed manually held records (paper systems). To gain access to ones data a written request should be made to ARBTA's Data Protection Officer along with proof of ID. The information will be provided within 28 working days of the request unless there is a reason for delay. Information held but provided by a third party will only be released on consent of its author, i.e. confidential references, the individual requesting access will need to gain this permission.

Data Transfer Outside the European Economic Area (EEA)

The 1998 Act restricts the transfer of data outside the EEA unless the country involved ensures an adequate level of 'data protection' along the lines outlined in this policy. ARBTA will satisfy itself

that any country outside the EEA has a equivalent approach to the UK before the transfer of data. Where there is any doubt of the veracity of another countries approach to data protection additional consent will need to be gained from the individual.

Any comments related to this policy should be sent in writing to:
The Data Protection Officer, ARBTA, 119 Oaklands Avenue, Oxhey Hall, Watford, Hertfordshire, WD19 4TN

Recommended	**GQAL**	**2022**
Approved	**Board of Directors**	**2022**
Next Review		**2024**

APPENDIX

GUIDANCE TO THE GENERAL DATA PROTECTION REGULATION (GDPR 2016)

All users of ARBTA's services should comply with the GDPR outlined in the following 12 steps of what this entails (taken from

Step 1 – Awareness
You should make sure that decisions makers and key people in your organization are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Step 2 – Information you hold
You should document what personal data you hold, where it came from, and who you share it with. You may need to organise an information audit.

Step 3 – Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Step 4 – Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Step 5 – Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide additional information.

Step 6 – Lawful basis for processing personal data
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Step 7 – Consent
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

Step 8 – Children
You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any processing activity.

Step 9 – Data breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Step 10 – Data protection by design and data protection impact assessments

Step 11 – Data protection officers
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

Step 12 – International
If your organisation operates in more that one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Further information can be gained from the Information Commissioners Officer (ICO) on www.ico.org.uk