

Rose Bruford College of Theatre and Performance

Data Protection Policy

1. Introduction

The College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example.

It is also necessary to process information in order that staff can be recruited and paid, programmes organised and legal obligations to funding bodies and government complied with.

Data in this context means means information

- which is processed by equipment operating automatically in response to instructions given for that person
- which is recorded with the intention that it should be processed by means of such equipment
- which is recorded as part of a relevant filing system or with the intention that it should be part of that system
- or is an accessible record such as a health, education, or other accessible public record

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, the College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary, these state that personal data shall be:

- Obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Adequate, relevant and not excessive for those purposes.
- Accurate and kept up to date.
- Kept for no longer than is necessary for that purpose.
- Processed in accordance with the data subject's rights.
- Kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.

2. Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with their line manager initially, who can raise it with Human Resources – for staff data, the Director of Finance for payroll information, and the Registrar - for student data. If the matter is not resolved it should be raised as a formal grievance.

3. The Data Controller and the Designated Data Controller/s

The College as a corporate entity is the data controller under the Act, and the Board of Governors is therefore ultimately responsible for implementation. However, the designated data controller is the Secretary & Registrar.

4. Notification of Data Held and Processed

All staff, students and other users are entitled to know

- What information the College holds and processes about them and why
- How to gain access to it.
- How to keep it up to date.
- What the College is doing to comply with its obligations under the 1998 Act.

The College will, therefore, provide all staff, students and other relevant users with a standard form of notification. This will state the types of data the College holds, the reasons why and manner in which it is processed.

The College will regularly review the data and reasons for which it is processed.

5. Responsibilities of Staff

All staff are responsible for

- Giving Rose Bruford College permission to process and store their information in line with published guidelines in order to pay them correctly, and manage the College correctly
- Checking that any information they provide to the College in connection with their employment and/or pay is accurate and up to date.
- Informing the College (in writing) of any changes to information as they occur e.g. changes of address.

- Checking the information that the College will send out from time to time, giving details of information kept and processed.
- Informing the College, in writing, of any errors or changes. The College cannot be held responsible for any errors if the staff member has not kept the information up to date.

If and when, as part of their responsibilities, staff collect information about others [i.e. students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances], they must comply with this policy.

6. Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on disk which is itself kept securely.

7. Students' Obligations

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc. are notified to the programme administrator or Registrar.

Students who use the College computer facilities may, from time to time, process personal data. If they do they must notify the data controller, i.e. the Registrar. Any student who requires further clarification about this should contact the Registrar or their Programme Administrator.

8. Rights to Access Information

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files.

Any student who wishes to exercise this right should complete the college "Access to Information" form and send it to the Registrar. Staff should contact Human Resources for their own information or Payroll using the "Right to Access" form.

The College is entitled to make a charge of £5 on each occasion that access is requested, although the College has the discretion to waive this charge.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the person making the request.

9. Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is College policy to make as much information public as possible, and in particular the following information will be available to the public for inspection.

- Names and contacts of College Governors
- List of staff
- Photographs of some staff
- Descriptions of key staff (e.g. skills, qualifications etc) on the web site

The College's internal phone list or intranet will not be a public document, but may be passed onto partner institutions.

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller who will consider the request.

10. Subject Consent

In many cases, the College can only process personal data with the consent of the individual.

In some cases, if the data is sensitive, **express written consent** must be obtained.

Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or programmes will bring the applicants into contact with children, including young people from the age of 8. The College has a duty under the Children's Act and other enactments to ensure that staff are suitable for the job, and students for the programme offered. The College also has a duty of care to all staff and students and must, therefore, make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will use the information in the protection of the health and safety of the individual, but will need consent to process it in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to sign a “Consent to Process” form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

11. Processing Sensitive Information

Sometimes it is necessary to process information about a person’s health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

12. Examination Marks

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the College.

13. Retention of Data

The College will keep some forms of information for longer than others. Because of storage limitations, information about students cannot be kept indefinitely, unless there are specific requests by the relevant authorities to do so.

13.1 Staff

The College will need to keep information about staff for long periods of time—sometimes over the entire employment of the employee of the College e.g. pensions. Further information is available from the HR Office.

13.2 Students

In general, detailed information about students will be kept for a maximum of three years after leaving the College. After this time, the College will only keep core information as follows:

- name and address,
- academic achievements, including marks for coursework and
- copies of any references written.

15. Responsibility for the update of this policy

The Secretary & Registrar will be responsible for the review and update of this policy, in line with changes to the legislation, and the needs of the College.

14. Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this Policy should be taken up with the designated data controller.