NEW LONDON PERFORMING ARTS CENTRE
DATA PROTECTION POLICY

The Data Protection Act 1998 is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Scope of the Policy

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The Centre collects a large amount of personal data every year including: staff records, names and addresses of those requesting information, examination marks, references, fee collection as well as the many different types of research data used by the Centre. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Eight Principles

The Act is based on eight data protection principles, or rules for 'good information handling'.

1. Data must be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specific and lawful purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

4. Personal data shall be accurate and where necessary kept up to date.

5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.

6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

3. Responsibilities

3.1 The Centre must:
Manage and process personal data properly
Protect the individual's right to privacy
Provide an individual with access to all personal data held on them.

3.2 The Centre has a legal responsibility to comply with the Act. The Centre is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

3.3 The Centre is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following link :
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

3.4 Every member of staff that holds personal information has to comply with the Act when managing that information.

3.5 The Centre is committed to maintaining the eight principles at all times. This means that the Centre will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice.

- check the quality and accuracy of the information held

- apply the records management policies and procedures to ensure that information is not held longer than is necessary

- ensure that when information is authorised for disposal it is done appropriately

- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system

- only share personal information with others when it is necessary and legally appropriate to do so

- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act **(See Annex A)**

- train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Annex A

New London Performing Arts Centre
Procedures for responding to requests to access personal information

CONTENT

1. INTRODUCTION

These procedures set out how to respond to requests for personal information from and about applicants, current and former students, staff and others whose personal data the Centre holds in accordance with their rights as data subjects under the Data Protection Act 1998 and the data protection laws of other relevant jurisdictions.

The scope of these procedures applies to information that we hold about all current and former New London Performing Arts Centre students or staff, regardless of where or how they studied or worked. These procedures support the Data Protection Policy and also other policies relating to the management of student and staff records.

2. REQUESTS BY CURRENT AND FORMER STUDENTS AND STAFF FOR THEIR OWN PERSONAL DATA

Everyone has the right to know what personal information organisations hold about them, why and how their information is held and used, with whom their information is shared and for what purpose and for how long their personal information is retained. People also have the right to check that the information held about them is accurate and to object to processing of information that would cause them damage and distress. In the Centre context, individuals may make requests for their own personal data which can be readily met in the normal line of business e.g. by asking for and receiving feedback on their progress or performance. The following procedures cover the most common scenarios for managing formal requests by individuals for their own personal data.

2.1 Handling Data Subject Access Requests

Under the UK Data Protection Act, a formal request for one's own personal data is called a data subject access request. However, people do not have to state that they are making a data subject access request, or cite the Data Protection Act, for their requests to be valid. A request by an individual for their own personal data may be simple or complex. The management of all such requests must be governed by a common set of rules.

2.2 All requests must be made in writing

We may not require anyone to complete a subject access request form but we can encourage people to use the form as it provides helpful prompts to focus the request and help staff identify where the relevant information is likely to be held. If someone asks for assistance in completing a request form, it can be helpful if the member of staff completes the form and asks the applicant to affirm that the details are correct and to sign it.

2.3 Proof of identification

If the person making the request for their own information (the data subject) is not known to the person receiving it, the data subject must provide proof of their identity in the form of their student ID card, a birth certificate, passport or driving licence.

2.4 Requests made on behalf of the data subject by a third party

If someone makes a request on behalf of another person e.g. a parent on behalf of their child or a lawyer on behalf of a client, the person making the request must provide evidence of their authority to make the request on behalf of the data subject, for instance confirmation of power of attorney, or the written consent of the data subject. If the officer receiving the request is in any doubt e.g. if the signature does not match those on record, it is necessary to contact the data subject to get confirmation of their consent to disclose their personal data to the third party. If the request is for information of a sensitive nature, it may be appropriate to send it to the data subject rather than the person making the request on their behalf.

2.5 Statutory timescales for complying with requests

The statutory deadline for responding to subject access requests is 40 calendar days from receipt of the request (and the fee if levied) or from confirmation of the identity of the person making the request. If the request is very vaguely worded, it is legitimate to stop the clock at the point that the original request is received in order to seek clarification of the information requested. The only exception to the 40 day deadline is where a student requests their marks or grades before the results have been announced. In this case, the deadline for providing the information is either 5 months of the date of the request or 40 days after the results have been announced, whichever is the earlier.

3 REQUESTS FOR PERSONAL DATA BY THIRD PARTIES

3.1 Under most circumstances we must obtain the written consent of individuals before disclosing their personal data to third parties.

3.2 **Third party requests to make contact with individuals**

In this context the personal data of current or former students includes the fact that they are or were a NLPAC student. If someone contacts the Centre asking to make contact with a current or former student or expressing concern about their welfare we must not confirm that the person is or was a student. We can offer to take the contact details of the enquirer and to forward these on to the individual concerned if our records confirm that they are or were at the centre, in order that the individual can chose whether to respond.

3.3 Disclosure of information about students to sponsors or employers

In some cases a student may have signed an agreement at enrolment consenting to the disclosure of limited personal data necessary to confirm their status, attendance, progress and awards to a sponsor or potential employer. If evidence of consent is on record, in such a case it is legitimate to disclose the information requested as long as it is possible to verify that the person making the request

- is who they claim to be,
- has the authority to make the request and
- has the consent of the applicant.

If in any doubt, seek the consent of the student.

3.4 Disclosure of information about staff: references

When receiving requests for references about a current or former member of staff it is legitimate for managers to disclose limited personal data necessary to verify the details of their employment and role at the Centre to a potential employer, as long as it is possible to verify that the person making the request

- is who they claim to be,
- has the authority to make the request and
- has the consent of the applicant.

If in any doubt, seek the consent of the data subject. Staff need to be aware that data subjects have the right to ask the organisation that receives the reference for a copy of it. Both organisations and data subjects have the right to take legal action against the authors of references where they consider that the reference has misrepresented the candidate's abilities.

3.5 When someone claims legal authority to request personal data

In some cases, requests for personal data may be received from people claiming legal authority to ask for the information concerned. In these cases recipients of requests should seek advice from the Centre Principal. Unless the person making the request has a warrant or court order requiring the Centre to disclose personal information about current or former students, the Centre is not obliged to comply with such requests. Therefore all staff who receive requests for personal data from the police or other government bodies must follow these procedures to ensure that disclosures of personal data are lawful, authorised, and accountable.

Requests from the Police - All requests for disclosure must be in writing, by email or letter. The request must

• be signed by an officer with the authority to make the request; this may be an electronic signature or a scanned image of a signed form, if the request is made by email.

• set out the legal authority for making the request. This is normally a specific section of the Data Protection Act.

The request must explain how this right applies and why they need the information. Even if the applicant is known to the person handling the request it is necessary to verify the applicant's identity and their authority to make the request.

3.6 Authorising disclosure to third parties

Requests to disclose personal data must be escalated to an officer who has designated authority to decide whether to release or withhold the information. For requests by the police, Home Office or other government bodies:

- For student personal data the responsible officer is the Office Manager.
- For staff personal data the responsible officer is the Office Manager.

The responsible officer will need to consider whether the disclosure is necessary for the purpose claimed e.g. the prevention or detection of crime or the apprehension or prosecution of offenders; not disclosing the personal data would be likely to prejudice the purpose cited. The responsible officer must be satisfied that the request is reasonable and proportionate and disclose only

the minimum personal data necessary for the purpose, seeking advice from the Principal as appropriate.

4 SECURITY OF COMMUNICATIONS

All personal data disclosed in response to a request must be communicated by a method appropriate to the security and sensitivity of the information. Before supplying information it is essential to check how the applicant wishes to receive the information and ensure that you have the correct postal or email address. Information containing sensitive personal data sent by email or using a USB memory stick or other portable media must be encrypted. If sending a hardcopy, then the packaging should be marked as strictly private and confidential and sent via recorded delivery.

5 KEEPING AN AUDIT TRAIL OF REQUESTS

All subject access requests and requests from third parties must be recorded on Centre systems so that the Centre has an audit trail of actions taken in response to a request and can justify each decision. The record must include details of the request, contact details of the applicant, evidence sought and obtained to verify their identity, the decision to release or withhold the information requested, the reasons for the decision and a copy of any information disclosed.

For requests by and about students: Straightforward subject access and third party requests must be recorded and kept in the student file. If the request is handled by the Centre and the student has left the Centre, the file should be retrieved from archive for the record to be added.

For requests by and about staff: Straightforward subject access and third party requests about current staff must be recorded in the individual's personal file. Where requests for information are received about former staff, the manager handling the request provide a record of the request and the response to add to the leaver's file.