LAINE

THEATRE ARTS

Policies

Data Protection Policy

DATA PROTECTION POLICY

This Policy sets out the obligations of Laine Theatre Arts Limited, a Company registered in the United Kingdom under number 01180133, and data protection registration reference: Z5943594, whose registered office is at 1st Floor Sheraton House, Lower Road Chorleywood, Rickmansworth, Hertfordshire, WD3 5LH regarding data protection and the rights of its data subjects in respect of their personal data under UK Data Protection Legislation (defined below).

This Policy sets out Laine Theatre Arts' obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to data subjects. The procedures and principles set out herein must be followed at all times by the College, its employees, agents, contractors, and other parties working on behalf of Laine Theatre Arts.

DEFINITIONS

College	Means Laine Theatre Arts Limited;
consent	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them;
Criminal Convictions Data	personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings;

Data controller	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, Laine Theatre Arts is the data controller of all personal data relating to data subjects;
Data processor	means a person or organisation which processes personal data on behalf of a data controller;
Data Protection Legislation	means all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation;
Data Protection Officer (DPO): either of the following:	a) the person required to be appointed in specific circumstances under the UK GDPR; or b) where a mandatory DPO has not been appointed, a data privacy manager or other voluntary appointment of a DPO or the Company data privacy team with responsibility for data protection compliance.

Data subject	means a living, identified, or identifiable individual about whom the college holds personal data;
EEA	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
Personal data	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
Processing	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise

	making available, alignment or combination, restriction, erasure or destruction;
Pseudonymisation	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;
Special category personal data	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

1. DATA PROTECTION OFFICER AND SCOPE OF POLICY

1.1. Laine Theatre Arts' Data Protection Officer is Sarah Carroll sarahcarroll@laine-theatre-arts.co.uk

The Data Protection Officer is responsible, together with the Executive Director, for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

1.2. The Principal, Executive Director, Director of Studies, Vice Principals and members of the Senior Management Team are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the College comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

1.3. Data protection is the responsibility of everyone within the College and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable the College to comply with applicable law. Compliance with this Data Protection Policy is mandatory.

1.4. This Data Protection Policy (together with any related policies or guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer.

1.5. Any questions relating to this Policy, Laine's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Data Protection Officer.

THE DATA PROTECTION PRINCIPLES

The Data Protection Legislation sets out the following principles with which anyone handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

1.6. processed lawfully, fairly, and in a transparent manner in relation to the data subject;

1.7. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

1.8. adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

1.9. accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

1.10. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject;

1.11. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

1.12. not transferred to another country without appropriate safeguards in place (transfer limitation);

1.13. made available to and allow data subjects to exercise certain rights in relation to their personal data.

2. THE RIGHTS OF DATA SUBJECTS

The Data Protection Legislation sets out the following key rights applicable to data subjects:

2.1. the right to withdraw consent at any time;

2.2. the right to be informed;

2.3. the right of access;

2.4. the right to rectification;

2.5. the right to erasure (also known as the 'right to be forgotten');

2.6. the right to restrict processing;

2.7. the right to data portability;

2.8. the right to object;

2.9. rights with respect to automated decision-making and profiling.

2.10. the right to request a copy of an agreement under which personal data is transferred outside of the UK;

2.11. the right to prevent processing that is likely to cause damage or distress to the data subject or anyone else;

2.12. the right to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

2.13. the right to make a complaint to the supervisory authority;

3. LAWFUL, FAIR AND TRANSPARENT DATA PROCESSING

3.1. The Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful only if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.2. If the personal data in question is special category personal data which shall include Criminal Convictions Data, (also known as 'sensitive personal data'), at least one of the following conditions must be met in addition to one of the conditions set out above:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);

b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

e) the processing relates to personal data which is manifestly made public by the data subject;

f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of

health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4. CONSENT

If consent is relied upon as the lawful basis for collecting, holding, and/or processing any personal data, the following shall apply:

4.1. Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

4.2. Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

4.3. Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

4.4. If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data

was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

4.5. Where special category personal data is processed, the College shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

4.6. In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the College can demonstrate its compliance with consent requirements.

4.7. In respect of any minor students, the College will at all times comply with all relevant laws and regulations concerning the controlling, processing and consent issues given the status of the College.

5. SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

5.1. The College collects and processes the personal data set out in Part 23 of this Policy. This includes:

a) personal data collected directly from data subjects and
b) personal data obtained from third parties.

5.2. The College only collects, processes, and holds personal data for the specific purposes set out in Part 23 of this Policy (or for other purposes expressly permitted by the Data Protection Legislation).

5.3. Data subjects shall be kept informed at all times of the purpose or purposes for which the College uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

6. ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING

6.1. The College will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in Part 23, below.

6.2. Employees, agents, contractors, or other parties working on behalf of the College may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

6.3. Employees, agents, contractors, or other parties working on behalf of the College may process personal data only when the performance of their job duties requires it. Personal data held by the College cannot be processed for any unrelated reasons.

7. ACCURACY OF DATA AND KEEPING DATA UP TO DATE

7.1. The College shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of an employee data subject, as set out in Part 17, below.

7.2. The accuracy of personal data shall be checked when it is collected and at twelve monthly intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7.3. It is the responsibility of individual data subjects to ensure that the personal data they have provided to the College is kept up to date. If any such personal data changes, employees should ensure that the relevant member of staff and/or department is informed as soon as is reasonably possible. The College relies on the cooperation of its employees to help meet its obligations under the Data Protection Legislation.

8. DATA RETENTION

8.1. The College shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which it was originally collected, held, and processed.

8.2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it securely and without delay.

8.3. For full details of the College's approach to data retention, including retention periods for specific personal data types held by the College, please refer to our Data Retention Policy.

9. SECURE PROCESSING

9.1. The College shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further

details of the technical and organisational measures which shall be taken are provided in the College's Data Security Policy.

9.2. All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

9.3. Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed;

c) authorised users must always be able to access personal data as required for the authorised purpose or purposes.

10. ACCOUNTABILITY AND RECORD KEEPING

10.1. The Data Protection Officer shall be responsible together with the HR Manager for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines

.

10.2. The College shall follow a 'privacy by design' approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).

10.3. All employees, agents, contractors, or other parties working on behalf of the College shall be given appropriate training in data protection and

privacy, addressing the relevant aspects of the Data Protection Legislation, this Policy, and all other applicable College policies.

10.4. The College's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

10.5. The College shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following:

a) the name and details of the College, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

b) the purposes for which the College collects, holds, and processes personal data;

c) the College's legal basis or bases (including, where applicable, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;

d) details of the categories of personal data collected, held, and processed by the College, and the categories of employee data subject to which that personal data relates;

e) details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;

f) details of how long personal data will be retained by the College (please refer to the College's Data Retention Policy);

g) details of personal data storage, including location(s);

h) detailed descriptions of all technical and organisational measures taken by the College to ensure the security of personal data.

11. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN

11.1. In accordance with 'privacy by design' principles, the College shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

11.2. The principles of 'privacy by design' should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose/purposes of the collection, holding and processing

b) the state of the art of all relevant technical and organisational measures to be taken;

c) the cost of implementing such measures; and

d) the risks posed to data subjects and to the College, including their likelihood and severity.

11.3. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed;

b) the purpose(s) for which personal data is to be used;

c) the College's objectives;

d) how personal data is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) the risks posed to data subjects;

h) the risks posed both within and to the College;

i) the proposed measures to minimise and handle identified risks.

12. KEEPING DATA SUBJECTS INFORMED

12.1. The College shall provide the information set out in Part 15.2 to every data subject:

a) Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the employee data subject, when the first communication is made;

ii) if the personal data is to be transferred to another party, before that transfer is made;

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2. The following information shall be provided in the form of a privacy notice:

a) details of the College including, but not limited to, all relevant contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 23 of this Policy) and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which the College is justifying its collection and processing of the personal data;

d) where the personal data is not obtained directly from the employee data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

f) where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 25 of this Policy for further details);

g) details of applicable data retention periods;

h) details of the data subject's rights under the Data Protection Legislation;

i) details of the data subject's right to withdraw their consent to the College's processing of their personal data at any time (where applicable);

j) details of the data subject's right to complain to the Information Commissioner's Office;

k) where the personal data is not obtained directly from the employee data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. DATA SUBJECT ACCESS

13.1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the College holds about them, what it is doing with that personal data, and why.

13.2. Data subjects wishing to make a SAR should do so using a Subject Access Request Form, sending the form to the College's Data Protection Officer at sarahcarroll@laine-theatre-arts.co.uk

13.3. Responses to SARs must normally be made within one month of receipt; however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4. All SARs received shall be handled by the College's Data Protection Officer in accordance with the College's Data Subject Access Request Policy and Procedure.

13.5. The College does not charge a fee for the handling of normal SARs. The College reserves the right to charge reasonable fees for additional copies of information that has already been supplied to an employee data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. RECTIFICATION OF PERSONAL DATA

14.1. Data subjects have the right to require the College to rectify any of their personal data that is inaccurate or incomplete.

14.2. The College shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the College of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. ERASURE OF PERSONAL DATA

15.1. Data subjects have the right to request that the College erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the College to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent (where applicable) to the College holding and processing their personal data;

c) the data subject objects to the College holding and processing their personal data (and there is no overriding legitimate interest to allow the College to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);

d) the personal data has been processed unlawfully;

e) the personal data needs to be erased in order for the College to comply with a particular legal obligation.

f) the personal data is being held and processed for the purpose of providing information society services to a child.

15.2. Unless the College has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's

request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3. In the event that any personal data that is to be erased in response to an data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. RESTRICTION OF PERSONAL DATA PROCESSING

16.1. Data subjects may, in certain limited circumstances, request that the College ceases processing the personal data it holds about them. If an employee data subject makes a valid request, the College shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. DATA PORTABILITY

17.1. The College processes personal data using automated means. Electronic filing.

17.2. Where data subjects have given their consent to the College to processing their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the

College and the data subject, data subjects have the right, under the Data Protection Legislation, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

17.3. To facilitate the right of data portability, the College shall make available all applicable personal data to data subjects in the following format:

a) Microsoft Word;

17.4. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

17.5. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. OBJECTIONS TO PERSONAL DATA PROCESSING

18.1. Data subjects have the right to object to the College processing their personal data based on legitimate interests, for direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

18.2. Where a data subject objects to the College processing their personal data based on its legitimate interests, the College shall cease such processing immediately, unless it can be demonstrated that the College's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

18.3. Where a data subject objects to the College processing their personal data for direct marketing purposes, the College shall cease such processing promptly.

18.4. Where a data subject objects to the College processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Data Protection Legislation, "demonstrate grounds relating to his or her particular situation". The College is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

18.5. The activities outlined in this are generally prohibited under the Data Protection Legislation where the resulting decisions have a legal or similarly significant effect on data subjects unless one of the following applies:

a) the data subject has given their explicit consent;

b) the processing is authorised by law; or

c) the processing is necessary for the entry into, or performance of, a contract between the College and the data subject.

18.6. If special category personal data is to be processed in this manner, such processing can only be carried out if one of the following applies:

d) the data subject has given their explicit consent; or
e) the processing is necessary for reasons of substantial public interest.

18.7. Where decisions are to be based solely on automated processing (including profiling), data subjects have the right to object, to challenge such decisions, request human intervention, to express their own point of

view, and to obtain an explanation of the decision from the College. Data subjects must be explicitly informed of this right at the first point of contact.

18.8. In addition to the above, clear information must be provided to data subjects explaining the logic involved in the decision-making or profiling, and the significance and envisaged consequences of the decision or decisions.

18.9. When personal data is used for any form of automated processing, automated decision-making, or profiling, the following shall apply:

a) appropriate mathematical or statistical procedures shall be used;

b) technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

c) all personal data to be processed in this manner shall be secured in order to prevent discriminatory effects arising.

19. PERSONAL DATA

The College collects, holds, and processes personal data about its employees at all times in accordance with data subjects' rights and the College's obligations under the Data Protection Legislation and this Policy.

For details of data retention, please refer to the College's Data Retention Policy.
Special Category Personal Data

19.1. Any and all special category (sensitive) personal data collected, held, and processed will be used strictly in accordance with the applicable conditions set out in Part 6 of this Policy.

19.2. Special category personal data shall be accessible and used only by the Principal or Executive Director to the extent strictly necessary to achieve the purpose(s) for which it is collected, held, and processed and shall not be revealed to other employees, agents, contractors, or other parties working on behalf of the College (except in exceptional circumstances where it is necessary to protect the vital interests of the employee data subject(s) concerned, and such circumstances satisfy the applicable conditions set out in Part 6 of this Policy).

IDENTIFICATION INFORMATION

19.3. The following identification information will be collected, held, and processed:

a) Name;

b) Contact details;

EMPLOYMENT RECORDS

19.4. The following information will be collected, held, and processed:

a) Interview notes;

b) CVs, application forms, covering letters, and similar documents;

c) Assessments, performance reviews, and similar documents;

d) Details of remuneration including salaries, pay increases, bonuses,

e) commission, overtime, benefits, and expenses;

f) Records of disciplinary matters including reports and warnings, both formal and informal;

g) Details of grievances including documentary evidence, notes from interviews, procedures followed, and outcomes;

EQUAL OPPORTUNITIES MONITORING

19.5. Equal opportunities monitoring information will be collected, held, and processed. Where possible, such data will be anonymised. The College will use special category personal data for equal opportunities monitoring only with data subjects' consent.

19.6. Such data will only be used to the extent required to reduce, stop, and prevent unlawful discrimination and to ensure that recruitment, promotion, training, development, assessment, benefits, pay, terms of employment, redundancy, and dismissals are determined on the basis of capability, qualifications, experience, skills, and productivity.

19.7. Data subjects may request that the College does not hold such data about them. All requests must be made in writing and addressed to the Data Protection Officer.

19.8. The following information will be collected, held, and processed:

a) Age;
b) Gender;
c) Ethnicity;
d) Nationality;
e) Religion;
f) Medical records where appropriate

HEALTH RECORDS

19.9. Health information will be collected, held, and processed where appropriate. Most health data constitutes special category (sensitive) personal data. The College will use special category personal data for health-related purposes only with data subjects' consent.

19.10. Health data will be only be used to the extent required to ensure that employees or students are able to perform their work or courses correctly, legally, safely, and without unlawful or unfair impediments or discrimination.

19.11. Data subjects may request that the College does not hold such data about them. All requests must be made in writing and addressed to the Data Protection Officer.

19.12. The following information will be collected, held, and processed:

a) Details of sick leave;
b) Medical conditions;
c) Disabilities;
d) Prescribed medication;

BENEFITS

19.13. If an employee is enrolled in a benefit scheme offered by the College, it may be necessary for third-party organisations to collect personal data from the employee. Any such employees will be provided with the necessary information prior to the collection of their data (as per the information requirements set out in Part 15 of this Policy).

19.14. The College shall not use any such personal data except to the extent necessary for the administration of the relevant benefits schemes.

19.15. Employees may request that the College does not supply their personal data to trade unions and shall be informed of that right before any transfer is made.

19.16. The following information may be supplied:

a) Name;
b) Job description;

EMPLOYEE MONITORING

19.17. The College may from time to time monitor employees' activities, such as internet and email monitoring. Unless exceptional circumstances (such as criminal investigations or matters of equal severity) justify covert monitoring, employees will be informed of any and all monitoring in advance. Monitoring shall not normally interfere with an employee's duties.

19.18. Monitoring will take place only if the College considers it necessary. Personal data collected for monitoring purposes will only be collected, held, and processed for reasons directly related to, and necessary for, achieving the intended result. Monitoring will always be conducted in accordance with employees' rights under the Data Protection Legislation.

19.19. Intrusion upon employees' personal communications and activities will be avoided whenever possible and under no circumstances will monitoring take place outside of an employee's normal place of work or working hours unless the employee is using College equipment or other

facilities such as College email, intranet, or a VPN provided by the College for its employees.

20. SHARING PERSONAL DATA

20.1. The College may only share personal data with third parties if specific safeguards are in place.

20.2. Personal data may only be shared with other employees, agents, contractors, or other parties working on behalf of the College if the recipient has a legitimate, job-related need-to-know. If any personal data is to be shared with a third party located outside of the UK, the provisions of Part 25, below, shall also apply.

20.3. Where a third-party data processor is used, that processor shall process personal data on behalf of the College (as data controller) only on the written instruction of the College.

20.4. Personal data may only be shared with third parties in the following circumstances:

a) the third party has a legitimate need to know the information for the purpose of providing services to the College under a contract;

b) the sharing of the personal data concerned complies with the privacy notice provided the affected data subjects (see Part 15 for more information) and, if required, the employees concerned have consented to the sharing of their personal data;

c) the third-party recipient has agreed to comply with all applicable data security standards, policies, and procedures, and has put in place adequate security measures to protect the personal data;

d) (where applicable) the transfer complies with any cross-border transfer restrictions (see Part 25, below);

e) a fully executed written agreement containing data processing clauses compliant with the Data Protection Legislation has been entered into with the third-party recipient.

21. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE OF THE UK

21.1. The College may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

21.2. Personal data may only be transferred to a country outside the UK if one of the following applies:

a) The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations'). From 1 January 2021, transfers of personal data from the UK to EEA countries will continue to be permitted. Transitional provisions are also in place to recognise pre-existing EU adequacy decisions in the UK.

b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.

c) The transfer is made with the informed and explicit consent of the relevant employee data subject(s).

d) The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the employee data subject and the College; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the employee data subject where the employee data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the College's legitimate interests.

22. DATA BREACH NOTIFICATION

22.1. All personal data breaches concerning personal data must be reported immediately to the College's Data Protection Officer.

22.2. If an employee, agent, contractor, or other party working on behalf of the College becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

22.3. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

22.4. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 26.3) to the rights

and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

22.5. Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the College's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the College to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

23. IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of 01/09/2023. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

KEY DATA

Version No:	4
Approved by:	Senior Management Committee
Review Interval:	3 Years
Last Review Date:	September 2023
Next Review Date:	August 2026
Owner:	Executive Director