TRINITY
COLLEGE LONDON

| TITLE | DATA PROTECTION POLICY |
|---|---|
| **Introduction** | 1.1 With effect from 25 May the General Data Protection Regulation ((EU) 2016/679) ('GDPR') replaces the EU Data Protection Directive 95/46/EC and supersedes the laws of individual Member States that were developed in compliance with the Directive. Its purpose is to protect the 'rights and freedoms' of living individuals and, in particular, to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.<br><br>1.2 The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system. It will apply to all data controllers and processors that are established in the European Union (EU) who process the personal data of data subjects, in the context of that establishment. It will also apply to data controllers and processors outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.<br><br>1.3 As noted above, the Data Protection Act 1998 is being repealed and will be replaced by new legislation to impose requirements in areas left to the discretion of Member States by the GDPR or not covered by it.<br>.<br>1.4 Article 4 definitions<br>For Article 4 definitions see Appendix 1 |
| **Policy Statement** | 2.1 Policy Statement<br><br>Trinity College London ('Trinity', 'us', 'we') is committed to compliance with all relevant EU and national laws in respect of personal data (including the GDPR and the UK implementing legislation (together referred to below as the 'Data Protection Laws')), and the protection of the 'rights and freedoms' of individuals whose information Trinity collects and processes.<br><br>Compliance with the GDPR is covered by this policy and other policies such as:<br>• Privacy Statement<br>• Data Retention Policy<br>• Data Destruction Policy<br>• Subject Access Request Procedure<br>• Information Security Policy |

| | |
|---|---|
| | The Data Protection Laws and this policy apply to all of Trinity's personal data processing functions including those performed on customers, clients' employees, suppliers and partners' data, and any other personal data the organisation processes from any source.<br><br>The Data Protection Officer is responsible for reviewing annually the processing register for any changes to Trinity's activities and to any additional requirements which have been identified by means of the data protection impact assessments. This register is available on the supervisory authority's request.<br><br>This Policy applies to all employees/staff of Trinity and therefore the Policy must be read and understood by every employee and contractor as part of their induction to Trinity.<br><br>Partners and any third parties working with or for Trinity, and who have or may have access to personal data, will be expected to have read, understood and comply with this policy. No third party may access personal data held by Trinity without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which than those which have been committed by Trinity, and which gives Trinity the right to audit compliance with the agreement.<br><br>2.2 How does this affect Trinity?<br><br>The use of personal data is critical to Trinity in order to:<br>• Recruit and pay staff<br>• Administer examination and award certificates<br>• Record progress<br>• Analyse and improve our service<br>• Collect fees<br>• Promote Trinity<br>• Comply with legal obligations to funding bodies and government<br><br>These activities, from start to finish, involve the use of personal data which will be covered by the GDPR.<br><br>2.3 The Policy applies to:<br>• Employees<br>• Council Members<br>• Contract, Freelance & Temporary staff<br>• Consultants and Advisers<br>• Examination Service Providers<br>• Examiners and Moderators<br>• National, Area and Local Area Representatives<br>• Registered Examination Centres and their Representatives<br>• Course Providers<br>• Third Parties that process data on behalf of Trinity |

| | |
|---|---|
| **Responsibilities** | 3.1 Responsibilities and roles under the Data Protection Laws<br><br>Trinity has a legal responsibility to comply with Data Protection Laws and treats compliance with its obligations seriously. We wish to obtain the highest possible standards to ensure that our internal procedures comply. We have developed the Policy to ensure that the Personal Data we collect and use is done so in accordance with the GDPR.<br><br>The Executive team and all those in managerial or supervisory roles within Trinity are responsible for developing and encouraging good information handling practices.<br><br>The Data Protection Officer is accountable for the management of personal data and has specific responsibilities for procedures such as the Subject Access Request Form and is the first point of contact for employees/staff seeking clarification on any aspect of data protection compliance.<br><br>All employees/staff are responsible for the compliance with Data Protection Laws and for ensuring that any personal data about them and supplied by them to Trinity is accurate and up-to-date. |
| **Data protection principles** | All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Trinity's policies and procedures are designed to ensure compliance with the principles.<br><br>4.1 <u>Personal data must be processed lawfully, fairly and transparently</u><br><br>The GDPR has increased requirements about what information should be available to data subjects. The specific information that must be provided to the data subject must, as a minimum, include:<br><br>• the identity and the contact details of the controller and, if any, of the controller's representative;<br>• the contact details of the Data Protection Officer;<br>• the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;<br>• the period for which the personal data will be stored;<br>• the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;<br>• the categories of personal data concerned;<br>• the recipients or categories of recipients of the personal data, where applicable;<br>• where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;<br>• any further information necessary to guarantee fair processing.<br><br>4.2 <u>Personal data can only be collected for specific, explicit and legitimate purposes</u> |

| | |
|---|---|
| | Data obtained for a specific purpose must not be used for a purpose that differs from the specified purpose. Details of how personal data is processed is set out in Trinity's **Privacy Statement.**<br><br>4.3 Personal data should be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed<br><br>The Data Protection Officer is responsible for ensuring Trinity does not collect information which is not strictly necessary for the purpose for which it is obtained. Please refer to the **Data Protection Impact Assessment (DPIA) Policy**.<br><br>All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a **Fair Processing Statement** or a link to Trinity's **Privacy Statement** and be approved by the Data Protection Officer.<br><br>The Data Protection Officer will ensure that all data collection methods are regularly reviewed to ensure that collected data continues to be adequate, relevant and not excessive. Please refer to the **Data Protection Impact Assessment (DPIA) Policy.**<br><br>4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay<br><br>Data stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.<br><br>The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.<br>It is also the responsibility of the data subject to ensure that data held by Trinity is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained on the application form is accurate at the date of submission.<br><br>Employees/staff, Contractors, Consultants, Examiners, Trinity representatives, centres plus any other third party are required to notify Trinity of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of Trinity to ensure that any notification regarding change of circumstances is recorded and acted upon.<br><br>The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.<br><br>On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by Trinity by referring to the data inventory. Any data that is no longer required in the context of the registered purpose will be identified in order for it |

| | |
|---|---|
| | to be securely deleted/destroyed in line with Trinity's **Data Destruction Policy**.<br><br>The Data Protection Officer is responsible for responding to any rectification requests from data subjects within one month. This is set out in the **Subject Access Request Procedure.** This can be extended to a further two months for complex requests. If Trinity decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.<br><br>Where third-party organisations may have been passed inaccurate or out-of-date personal data, the Data Protection Officer is responsible for making appropriate arrangements to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.<br><br>4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.<br><br>Personal data will be retained in line with the **Data Retention Procedure** and, once its retention date is passed, it must be securely destroyed as set out in this procedure.<br><br>The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in the **Data Retention Policy**, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be in writing.<br><br>4.6 Personal data must be processed in a manner that ensures appropriate security<br><br>The Data Protection Officer will undertake a risk assessment to take into account all the circumstances of Trinity's controlling or processing operations.<br><br>In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Trinity, and any likely reputational damage.<br><br>When assessing appropriate technical measures, the following will also be considered:<br>• Password protection;<br>• Automatic locking of idle terminals;<br>• Removal of access rights for USB and other memory media;<br>• Virus checking software and firewalls;<br>• Role-based access rights including those assigned to temporary staff;<br>• Encryption of devices that leave the organisations premises such as laptops; |

| | |
|---|---|
| | • Security of local and wide area networks;<br>• Privacy enhancing technologies such as pseudonymisation and anonymisation;<br>• Identifying appropriate international security standards relevant to Trinity<br><br>When assessing appropriate organisational measures, the following will be considered:<br>• The appropriate training levels throughout Trinity;<br>• Measures that consider the reliability of employees (such as references etc.);<br>• The inclusion of data protection in employment contracts;<br>• Identification of disciplinary action measures for data breaches;<br>• Monitoring of staff for compliance with relevant security standards;<br>• Physical access controls to electronic and paper based records;<br>• Adoption of a clear desk policy;<br>• Storing of paper based data in lockable fire-proof cabinets;<br>• Restricting the use of portable electronic devices outside of the workplace;<br>• Restricting the use of employee's own personal devices being used in the workplace;<br>• Adopting clear rules about passwords;<br>• Making regular backups of personal data and storing the media off-site;<br>• The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.<br><br>These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.<br><br>4.7 <u>The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)</u><br><br>The GDPR includes provisions that promote accountability and governance. Trinity will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection, DPIAs, breach notification procedures and incident response plans. |
| **Data subjects' rights** | 5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:<br>• To make subject access requests regarding the nature of information held about them and to whom it has been disclosed.<br>• To prevent any processing that is likely to cause damage or distress.<br>• To prevent processing for purposes of direct marketing.<br>• To be informed about the mechanics of automated decision-taking process that will significantly affect them.<br>• To not have significant decisions that will affect them taken solely by automated process. |

| | |
|---|---|
| | • To sue for compensation if they suffer damage by any contravention of the GDPR.<br>• To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.<br>• To request the supervisory authority to assess whether any provision of the GDPR has been contravened.<br>• To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.<br>• To object to any automated profiling that is occurring without consent.<br><br>5.2 Trinity ensures that data subjects may exercise these rights:<br>• Data subjects may make data access requests as described in the **Subject Access Request Procedure**; this procedure describes how Trinity will ensure that its response to the data access request complies with the requirements of the GDPR.<br>• Data subject have the right to complain to Trinity with regards to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the **Complaints Procedure**. |
| **Consent** | 6.1 Trinity understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, that it signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.<br><br>6.2 Trinity understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.<br><br>6.3 To demonstrate consent, there must be some active communication between the parties concerned. To demonstrate active consent, consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.<br><br>6.4 For sensitive data, explicit written consent must be obtained unless an alternative legitimate basis for processing exists.<br><br>6.5 Where Trinity provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13). |

| | |
|---|---|
| **Legitimate Interest** | 7. 1 Where Trinity does not engage directly with children, parents or guardians, it may rely on their implied consent for the processing of personal data and will only collect, store and process personal data that are necessary for the delivery of their exams and to meet regulatory requirements concerning those exams. |
| **Security of data** | 8.1 All Employees/Staff are responsible for ensuring that any personal data that Trinity holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Trinity to receive that information and has entered into a confidentiality agreement.<br><br>8.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with Trinity's **Access Control Policy**. All personal data should be treated with the highest security and kept securely e.g in a locked drawer or filing cabinet or if computerised password protected. Any data that needs to be destroyed, needs to be done so in line with Trinity's **Data Destruction Policy.** |
| **Disclosure of data** | 9.1 Trinity must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and in certain circumstances, the police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Trinity's business.<br><br>9.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer. For guidelines please refer to the **Subject Access Request Procedure**. |
| **Retention and disposal of data** | 10.1 Trinity shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.<br><br>10.2 Trinity may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.<br><br>10.3 The retention period for personal data will be set out in the Data Retention Procedure including any statutory obligations Trinity has to retain the data.<br><br>10.4 Trinity's **Data Retention** and **Data Destruction Policy** will apply in all cases.<br><br>10.5 Personal data must be disposed of securely in accordance with the GDPR's sixth principle, processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of |

| | |
|---|---|
| | data subjects. Any disposal of data will be done in accordance with the **Data Destruction Policy**. |
| **Data transfers** | 11.1 The GDPR imposes restrictions on the transfer of personal data outside the EU, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.<br><br>11.2 Transfers may be made where the EU Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.<br><br>See Appendix 2, for details of specified safeguards or exceptions. |
| **Effective Date** | April 2018 |
| **Date of next review** | April 2019 |

**Document Owner and Approval**
The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements.

This policy was approved by Trinity's Executive on 11 May 2018 and is issued on a version controlled basis.

**APPENDIX 1**

Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject') is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on 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.

Profiling **–** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach **–** 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Child **–** the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of

a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Supervisory Authority – is the Information Commissioner's Office (ICO) in the UK.

**APPENDIX 2**

Details of specified safeguards or exceptions.

**An adequacy decision**
The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/internationaltransfers/adequacy/index_en.htm*

**Privacy Shield**
If Trinity wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.

Assessment of adequacy by the data controller
In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:
- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

**Binding corporate rules**
Trinity may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Trinity is seeking to rely upon.

**Model contract clauses**
Trinity may adopt approved model contract clauses for the transfer of data outside of the EEA. If Trinity adopts a model contract there is an automatic recognition of adequacy.

**Exceptions**

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.