TRINITY
COLLEGE LONDON

TITLE	DATA PROTECTION POLICY
Introduction	1.1 With effect from 25 May 2018 the General Data Protection Regulation ((EU) 2016/679) ('**GDPR**') replaced the EU Data Protection Directive 95/46/EC ('**Directive**') and superseded the laws of individual EU member states ('**Member States**') that were developed in compliance with the Directive. The purpose of the GDPR is to protect the 'rights and freedoms' of living individuals and, in particular, to ensure that their Personal Data is not processed without their knowledge, and, wherever possible, that it is processed with their consent. 1.2 The GDPR applies to the Processing of Personal Data wholly or partly by automated means (eg. by a computer) and also other than by automated means (eg. paper records that form part of, or are intended to form part of, a Filing System). It applies to all Data Controllers and Data Processors that are established in the European Union (EU) who process the Personal Data of Data Subjects in the context of that establishment. It also applies to Data Controllers and Data 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are resident in the EU. 1.3 As a consequence of the GDPR coming into effect, the UK Data Protection Act 1998 has been repealed and replaced by the UK Data Protection Act 2018. Amongst other elements, the Data Protection Act 2018 legislates for areas left to the discretion of Member States by the GDPR or not covered by the GDPR. In this policy, the GDPR and the Data Protection Act 2018 shall be together referred to as the 'Data Protection Laws'. 1.4 Capitalised terms used in this policy and not otherwise defined within this policy shall have the meanings given to them in Appendix 1. 1.5 The UK left the EU on 31 January 2020 and is in a transition period until 31 December 2020 ('**Transition Period**'). At the end of the Transition Period there will be no changes to the applicability of the GDPR in the UK as the GDPR has been incorporated into UK law.
Policy Statement	2.1 Policy Statement Trinity College London (together with its wholly owned subsidiaries, '**Trinity**', '**us**', '**we**') is committed to: • compliance with the Data Protection Laws and all other relevant EU and national laws in respect of Personal Data; and • the protection of the rights and freedoms of individuals whose information Trinity collects and processes.

Trinity's compliance with the Data Protection Laws is covered by this policy and other policies such as:

- Privacy Statements;
- Data Retention Policy;
- Data Retention Schedule;
- Data Destruction Policy;
- Data Protection Impact Assessment Policy;
- Data Subject Access Request Policy;
- Information Security Policy;
- Personal Data Complaints Procedure; and
- Cookie Policies.

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' Personal Data, and any other Personal Data from any source that Trinity processes.

The Data Protection Officer is responsible for reviewing annually the Processing register for any changes to Trinity's activities and for 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.

This policy applies to all staff of Trinity and therefore must be read and understood by every employee and contractor as part of their induction to Trinity.

Partners and any other Third Parties working with or for Trinity, and who may be reasonably expected to have access to Personal Data, will be expected to read, understand and comply with this policy. No Third Party may access Personal Data held by Trinity without having first entered into a data confidentiality agreement with Trinity which:

- imposes on the Third Party obligations no less onerous than those which have been committed to by Trinity; and
- gives Trinity the right to audit compliance with the agreement.

2.2 <u>How does this policy affect Trinity?</u>

The use of Personal Data is critical to Trinity in order to:

- recruit and pay staff;
- administer examinations and award certificates;
- record progress;
- analyse and improve our service;
- collect fees;
- promote Trinity; and
- comply with legal obligations, including to regulatory and other government bodies.

To carry out these activities, Trinity collects and processes Personal Data. Set out in this policy is an explanation of how Trinity collects, processes and safeguards Personal Data in accordance with the Data Protection Laws.

2.3 This policy applies to:

- employees;
- council members;

	• contract, freelance and temporary staff; • consultants and advisers; • examination and other service providers; • examiners, stewards and moderators; • national, area and local area representatives; • registered examination centres and their representatives; • course providers; and • Third Parties that process data on behalf of Trinity.
Responsibilities	3.1 Responsibilities and roles under the Data Protection Laws Trinity has a legal responsibility to comply with the Data Protection Laws. We take this responsibility seriously and have developed this policy to ensure that we collect, use and safeguard Personal Data in accordance with the Data Protection Laws. The Executive team and all those in managerial or supervisory roles within Trinity are responsible for developing and encouraging good data handling practices. The Data Protection Officer is accountable for the management of Personal Data and is the first point of contact for staff or Third Parties seeking clarification on any aspect of data protection compliance. The Data Protection Officer also has specific responsibilities for procedures such as handling Data Subject access requests. All staff are responsible for 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 these principles. 4.1 Personal Data must be processed lawfully, fairly and transparently (Lawfulness, Fairness and Transparency) 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: • the identity and the contact details of the Data Controller and, if any, of the Data Controller's representative; • the contact details of the Data Protection Officer; • the purposes of the Processing for which the Personal Data is intended as well as the legal basis for the Processing; • the period for which the Personal Data will be stored; • the existence of the rights of Data Subjects 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; • the categories of Personal Data concerned; • the recipients or categories of recipients of the Personal Data, where applicable;

- where applicable, that the Data Controller intends to transfer Personal Data to a recipient in a third country and the level of protection afforded to the data; and
- any further information necessary to guarantee fair Processing.

The GDPR provides specific basis for Processing, some of which are set out below:

- the Data Subject has given his or her consent;
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests; or
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

Further information on some of these are set out in the sections of this policy on 'Consent', 'Legal Obligation', 'Contractual Relationship' and 'Legitimate Interest'.

4.2 Personal Data can only be collected for specific, explicit and legitimate purposes (Purpose Limitation)

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.**

4.3 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation)

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**.

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.

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.**

4.4 Personal Data must be accurate and kept up to date with every effort to erase or rectify without delay (Accuracy)

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.

The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

	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. Employees, contractors, consultants, examiners, Trinity representatives, centres plus any other Third Parties 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. 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 data might change and any other relevant factors. 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**. The Data Protection Officer is responsible for responding to any rectification requests from Data Subjects within one month. This is set out in the **Data Subject Access Request Policy.** 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 a judicial remedy. 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 such Third Party that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and • passing on any correction to the Personal Data to the Third Party where this is required. 4.5 <u>Personal Data must be kept in a form such that the Data Subject can be identified only as long as is necessary for Processing (Storage Limitation).</u> Personal Data will be retained in line with the **Data Retention Policy** and, once its retention date is passed, it must be securely destroyed as set out in that policy. 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 Laws. This approval must be in writing. 4.6 <u>Personal Data must be processed in a manner that ensures appropriate security (Security, Integrity and Confidentiality)</u> Personal Data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect

against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

The Data Protection Officer will undertake a risk assessment to take into account all the circumstances of Trinity's Processing operations.

In determining appropriateness of the technical and organisational measures required to protect Personal Data, the Data Protection Officer should 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.

When assessing appropriate technical measures, the following will also be considered:

- password protection;
- automatic locking of idle terminals;
- removal of access rights for USB and other memory media;
- virus checking software and firewalls;
- role-based access rights including those assigned to temporary staff;
- encryption of devices that leave Trinity's premises such as laptops;
- security of local and wide area networks;
- privacy enhancing technologies such as pseudonymisation and anonymisation; and
- identifying appropriate international security standards relevant to Trinity.

When assessing appropriate organisational measures, the following will be considered:

- the appropriate training levels throughout Trinity;
- measures that consider the reliability of employees (such as references etc.);
- the inclusion of data protection in employment contracts;
- identification of disciplinary action measures for data breaches;
- monitoring of staff for compliance with relevant security standards;
- physical access controls to electronic and paper based records;
- adoption of a clear desk policy;
- storing of paper based data in lockable fire-proof cabinets;
- restricting the use of portable electronic devices outside of the workplace;
- restricting the use of staff's own personal devices being used in the workplace;
- adopting clear rules about passwords;
- making regular backups of Personal Data and storing the media off-site; and
- the imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to Personal Data, the nature of Personal Data to be protected, and the potential for damage or distress to individuals whose data is being processed.

4.7 <u>Personal Data must not be transferred to another country without appropriate safeguards being in place (Transfer Limitation)</u>

	This principle is more fully covered under the section on 'Data Transfers' later in this policy. 4.8 Personal Data should be made available to Data Subjects and Data Subjects should be allowed to exercise certain rights in relation to their Personal Data (Data Subjects' Rights and Requests). This principle is more fully covered under the next section on 'Data Subjects' rights'. 4.9 The Data Controller is responsible for and must be able to demonstrate compliance with the principles listed in this section (Accountability) The GDPR includes provisions that promote accountability and governance. Trinity will demonstrate compliance with the data protection principles by appointing a suitably qualified Data Protection Officer, implementing data protection policies, adhering to codes of conduct, providing regular training on data protection to staff and other relevant personnel, regularly testing privacy measures implemented and conducting periodic reviews and audits to assess compliance, implementing technical and organisational measures, as well as adopting techniques such as data protection impact assessments, privacy by design, breach notification procedures and incident response plans.
Data Subjects' rights	5.1 Data Subjects have rights regarding data Processing, and the Personal Data that is recorded about them. These include rights to: • withdraw consent to the Processing of their Personal Data at any time (further details on consent are covered in the section of this policy on 'Consent'); • receive certain information about the Processing of their Personal Data; • make subject access requests regarding the nature of information held about them and to whom it has been disclosed (further details on subject access requests are covered in the section of this policy on 'Data Subject access requests'); • prevent any Processing that is likely to cause damage or distress; • prevent Processing for purposes of direct marketing; • restrict Processing in specific circumstances; • be informed about the mechanics of any automated decision-taking process that will significantly affect them; • not have significant decisions that will affect them taken solely by automated process; • sue for compensation if they suffer damage by any contravention of the GDPR; • request a copy of an agreement under which Personal Data is transferred outside of the EEA; • take action to rectify inaccurate data, erase Personal Data if it is no longer necessary for the purposes for which it was collected, or complete incomplete Personal Data (for further details see the section on 'Data erasure' in this policy; • request the Supervisory Authority to assess whether any provision of the GDPR has been contravened; • be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

	• make a complaint to the Supervisory Authority; • have Personal Data provided to them in a structured, commonly used and machine-readable format, and to have that data transmitted to another Data Controller; and • object to any automated Profiling that is occurring without consent. 5.2 Trinity ensures that Data Subjects may exercise these rights through the following: • Data Subjects may make data access requests as described in the **Data Subject Access Request Policy** (further details on subject access requests are covered in the section of this policy on 'Data Subject access requests'); and • Data Subjects 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 **Personal Data Complaints Procedure**.
Consent	6.1 Trinity understands 'consent' of the Data Subject to mean any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which the Data Subject, by statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her. The Data Subject can withdraw their consent at any time and must be able to do so easily. 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. 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. 6.4 For Special Categories of Personal Data, explicit written consent must be obtained unless an alternative basis for Processing exists. Where Processing of Special Categories of Personal Data is on the basis of explicit written consent, then Trinity must issue a privacy notice to the Data Subject. 6.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to capture and keep records of all consents received and withdrawn so that Trinity can demonstrate compliance with the GDPR.
Legal Obligation	7.1 Trinity can use this basis of Processing to comply with a common law or statutory obligation that Trinity is subject to where the Processing of Personal Data is necessary in order to comply. For example, Trinity processes Personal Data of candidates to comply

		with Trinity's obligation to provide reasonable adjustments to candidates with disability.
	7.2	Trinity should document any decision to rely on this lawful basis and should be able to identify the specific legal provision or an appropriate source of advice or guidance that sets out the legal obligation concerned.
Contractual Relationship	8.1	Trinity can use this basis of Processing a person's Personal Data to deliver a contracted service to them or because they have asked Trinity to do something before entering into a contract. The Processing must be necessary and Trinity should document when this lawful basis of Processing is relied upon.
Legitimate Interest	9.1	Data Protection Laws allow Trinity to collect and use personal information where Trinity uses people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the Processing.
	9.2	Where Trinity relies on legitimate interests to process data, Trinity must: • identify a legitimate interest (Trinity's own interest or the interests of Third Parties); • show that the Processing is necessary to achieve it; and • balance it against the individual's interests, rights and freedoms.
	9.3	For example, it is in Trinity's legitimate interest to process Personal Data of any person who contacts Trinity with an enquiry in order to respond to such enquiry, or when Trinity makes recordings of its examinations in order to monitor quality of its assessments and/or for research and training.
	9.4	Trinity must keep a record of the legitimate interests' assessments carried out to help demonstrate compliance if required. Details of the legitimate interests should also be included in the privacy statement.
Security of data	10.1	All staff must comply with all applicable sections of Trinity's **Information Security Policy**. In addition to complying with the measures described in paragraph 4.6 of this policy, all staff are responsible for protecting any Personal Data that Trinity holds and are to follow all security measures adopted by Trinity: • to maintain the security of all Personal Data; • against unlawful or unauthorised Processing of Personal Data; and • against the accidental loss of, or damage to, Personal Data.
	10.2	Staff are responsible for exercising particular care in protecting Special Categories of Personal Data from loss and unauthorised access, use or disclosure. Staff must ensure that Personal Data is not disclosed to any Third Party unless that Third Party has been specifically authorised by Trinity to receive such Personal Data and has entered into a confidentiality agreement with Trinity.
	10.3	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, for example 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	11.1	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 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.
	11.2	All requests to provide data to a third party 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 **Data Subject Access Request Policy**.
Retention and disposal of data	12.1	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.
	12.2	Trinity may store Personal 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.
	12.3	The retention period for Personal Data will be set out in the **Data Retention Policy** including any statutory obligations Trinity has to retain the data.
	12.4	Personal Data must be disposed of securely in accordance with the GDPR. Trinity's **Data Retention Policy** and **Data Destruction Policy** will apply in all cases.
Data erasure	13.1	Data Subjects have the right to have their inaccurate Personal Data erased. This is also known as 'the right to be forgotten'. It is not, however, an absolute right and applies in the circumstances listed below. Data Subjects also have the right for inaccurate Personal Data to be rectified or completed (if it is incomplete).
	13.2	Trinity is not required to rectify or erase Personal Data of a Data Subject where to do so would prevent the Data Subject from meeting their contractual obligations to Trinity or where Trinity is required to process (including retaining) such Personal Data for a lawful purpose in accordance with the Data Protection Laws.
	13.3	Individuals have the right to have their Personal Data erased if: • the Personal Data is no longer necessary for the purpose for which it was originally collected or processed; • Trinity is relying on consent as the lawful basis for holding the data, and the person withdraws their consent; • the Personal Data has been unlawfully processed; or

	• Trinity is relying on legitimate interest as the basis for Processing, the individual objects to the Processing of their data, and there is no overriding legitimate interest to continue this Processing. 13.4 Where Personal Data is erased, Trinity will search databases and other systems and applications where the Personal Data may be held and erase it within 1 month from the date of the request. 13.5 In the case of rectifying inaccurate Personal Data, Trinity must rectify the information without delay and notify the Data Subject that this has been completed within one month using the same procedures as for a data subject access request as set out in the **Data Subject Access Request Policy**.
Data Subject access requests	14.1 Subject to certain statutory exceptions, Data Subjects have the right to request confirmation that we process their Personal Data, obtain certain information about the processing of their Personal Data by Trinity and obtain a copy of the Personal Data processed. Data Subjects can make data access requests following the procedure set out in the **Data Subject Access Request Policy**. The **Data Subject Access Request Policy** describes how Trinity will ensure that its response to data access requests complies with the requirements of the GDPR. 14.2 As noted, exemptions may apply. For example, under Data Protection Laws, Trinity is not required to provide Personal Data comprising information recorded by candidates during examinations and/or in circumstances where its release would adversely affect our rights in the intellectual property and confidentiality of our examinations or reveal the Personal Data of another Data Subject. Accordingly, where necessary for these reasons, Trinity may withhold or obscure parts of recordings or examination scripts when responding to a subject access request.
Data transfers	15.1 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. 15.2 Transfers of Personal Data outside the EU can only take place where a condition set out in Appendix 2 to this policy applies. See Appendix 2 for details of specified safeguards or exceptions. 15.3 At the end of the Transition Period, transfers of Personal Data from the UK to the EEA will not be restricted. The existing restrictions on the transfer of Personal Data out of the EU will apply for transfers of Personal Data from the EEA to the UK.
Reporting a Personal Data Breach	16.1 All staff should be aware that any breach of Data Protection legislation may result in Trinity's disciplinary procedures or termination proceedings being instigated, as appropriate. 16.2 The GDPR requires Trinity to notify any Personal Data Breach to the Supervisory Authority and, in certain instances, the Data Subject.

	16.3 Trinity has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so. 16.4 If a Personal Data Breach has occurred or is suspected to have occurred, staff must not attempt to investigate the matter themselves but should immediately contact the Data Protection Officer. Staff should preserve all evidence relating to the potential Personal Data Breach.
Effective Date	April 2018 amended September 2020
Date of next review	September 2021

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

DEFINITIONS AND TERMS

Child, Children **–** the GDPR refers to a child as being anyone under the age of 16 years old, although this may be lowered to 13 years old or above by Member State law (and has been lowered to 13 years old in the UK). The Processing of Personal Data of a child is only lawful if parental or custodian consent has been obtained. The Data 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.

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 data controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor – means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

Data Subject – any living identified or identifiable natural person 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.

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.

Personal Data – any information relating to a Data Subject.

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 Data Controller to report Personal Data Breaches to the Supervisory Authority where the breach is likely to adversely affect the Personal Data or privacy of the Data Subject.

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, health, personal preferences, interests, reliability, behaviour, location or movements. 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.

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.

Supervisory Authority – means an independent public authority which is established by a Member State pursuant to the GDPR. In the UK the Supervisory Authority is the Information Commissioner's Office (ICO).

Third Party – a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process Personal Data.

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 for the transfer of Personal Data.

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/international-transfers/adequacy/index_en.htm*

Binding corporate rules

Trinity may adopt approved binding corporate rules for the transfer of Personal 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 or Standard Contractual Clauses (SCCs)

Trinity may adopt approved SCCs for the transfer of Personal Data outside of the EEA. Trinity is responsible for assessing whether Personal Data transferred to the third country receives protection 'essentially equivalent' to that provided under EU law in order to determine if the guarantees provided by the SCCs can be complied with in practice.

In making this assessment, Trinity 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 security measures that are to be taken as regards the Personal Data in the overseas location;
- access to Personal Data by public authorities (whether provided for in law, whether there are limits on such access, whether it is necessary and proportionate);
- availability of enforceable rights and effective legal remedies for Data Subjects; and
- other relevant aspects of the legal system, particularly those set out in Article 45(2) of the GDPR (eg. adequacy of privacy laws, the existence and effective functioning of an independent supervisory authority with adequate enforcement powers, international commitments and instruments entered into by the third country particularly in relation to the protection of Personal Data).

Exceptions

In the absence of an adequacy decision, 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 Data 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 Data 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.