TRINITY
COLLEGE LONDON

Trinity College London

Data Protection Policy

[April 2011]

CONTENTS

APPENDICES

1. INTRODUCTION

1.1 Trinity College London (Commitment)

Trinity College London ("Trinity", "us", "we") is committed to a policy of protecting the rights and privacy of all individuals from whom personal data is collected and used (this includes candidates, employees, job applicants, examiners, contractors and other business and professional contacts, trustees, staff and other individuals – the "individuals") in accordance with the Data Protection Act 1998 ("the Act").

Trinity needs to collect and process certain information about individuals for a range of operational purposes (e.g. to recruit and pay staff, to administer examinations, to agree awards and to collect fees).

Everyone in Trinity is accountable for upholding the requirements of this Data Protection Policy ("Policy") and therefore the Policy must be read and understood by every employee and contractor as part of their induction to Trinity.

This Policy should also be read by those listed in section 1.3 below.

The Policy covers the use of personal data about the individuals listed above and should be read in conjunction with any other policies and procedures of Trinity from time to time in place, including ("related policies"):

- Information Security Policy
- Data Retention Policy
- HR Data Protection – Staff
- HR Data Protection - Recruitment
- Subject Access Request Procedure

We need to comply with the rules set out in the Policy about how we use Personal Data. No one is exempt from compliance with these rules.

1.2 What does the Data Protection Act 1998 do?

The purpose of the Act is to give people the right to control how their "Personal Data" (any information that relates to them, such as a name, contact details, allegations of criminal activity, preferences, etc.) is used.

All EU countries have national laws that reflect the EU Data Protection legislation. However, the majority countries in Trinity markets (with the exception of Argentina, Canada, Guernsey, the Isle of Man and Switzerland) do not have data protection legislation in place that provides the same level of protection afforded by European data protection legislation.

Further information about how to carry out international transfers lawfully can be found in Section 2, Rule 8 of this Policy.

1.3 How does this affect Trinity?

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

- recruit and pay staff
- administer examinations and agree awards
- record progress
- analyse and improve our service
- collect fees
- promote Trinity, and
- comply with legal obligations to funding bodies and government

Further information about the purposes for which each department in Trinity processes Personal Data can be found in Appendix 1.

These activities, from start to finish, involve the use of Personal Data which will be covered by the Act.

Trinity will also use Personal Data given to Trinity by other organisations e.g. Trinity Laban.

The Policy applies to:

- Employees
- Council members
- Contract, freelance staff & temporary staff
- Consultants
- Examination Service Providers
- Examiners
- National, Area and Local Area Representatives
- Registered Examination Centres and their representatives
- Course Providers
- Third parties that process data on behalf of Trinity

1.4 What is Trinity doing about it?

Trinity 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 Act.

1.5 Responsibilities

Trinity has a legal responsibility to comply with the Act. The Director with overall responsibility for this Policy is the Director of Operations & IT (Richard Michel).

Other key roles:

Council

Trinity's Council members have overall responsibility for ensuring that Trinity complies with its legal obligations.

Data Protection Officer

The responsibilities of this post are described in Appendix 2.

Team/Department Managers

Each team or department manager should be responsible for ensuring that the members of their team comply with this Policy and the related policies.

Any issues related to the practical implementation of this Policy should be discussed with the Data Protection Officer.

Registered Examination Centres, Course Providers and Representatives of Trinity

In relation to candidate data, registered examination centres and representatives must follow the instructions set out in the contract (including any operational handbook) that they enter into with Trinity.

1.6 What are the consequences if Trinity gets it wrong?

Getting it wrong is serious for our business. It could also lead to complaints from individuals, compensation claims, fines from the Information Commissioner ("ICO") and bad publicity for Trinity.

1.7 Why is the Policy important to Trinity?

It is vital that those working in or for Trinity observe the Policy, since the collection and use of Personal Data is part of our everyday business. Likewise, we must ensure that we use the information we hold on individuals in accordance with the Act. The Policy sets out the standards that all those working in Trinity must adhere to.

1.8 Want more information?

If you want more information about data protection please contact the Data Protection Officer.

2. RULES

All processing of Personal Data must be done in accordance with the rules set out below which reflect the eight data protection principles in the Act.

Rule 1: Ensuring transparency

We must be transparent about the Personal Data that we hold on individuals.

Understanding the Rule

Being open and transparent in the way organisations use and share Personal Data is an important step to demonstrate good data protection practices. Trinity is subject to this requirement in how it uses Personal Data. As such, individuals should be properly notified.

Practical Steps

Fair processing information notices providing information about how Trinity uses the Personal Data must be provided to individuals, if possible at time of collection of that information (e.g. application forms, webforms, contractual clauses, surveys, syllabuses, etc) or as soon as practicable after that.

Candidates will receive this information via the Registered Examination Centres or from Trinity.

Trinity's employees and contractors should also be provided with a fair processing information notice in their contracts.

Rule 2: Using Personal Data for a justifiable purpose only

We must only obtain and use Personal Data for purposes which are lawful and justifiable.

Understanding the Rule

Trinity must only collect the Personal Data of individuals where it is relevant to its activities.

This rule means that we must identify and publicise the purposes for which Personal Data will be processed in the documents used at the time of collection (or soon after) in order to notify individuals.

Personal information shall not be used in a manner incompatible with the purpose for which it was obtained.

Practical Steps

When collecting Personal Data from individuals, we must ensure that the fair processing information notice made available to those individuals contains all of the purposes for which the Personal Data may be used.

In addition, when collecting information, we must only collect those details which are necessary for the purposes for which that information is being obtained.

Rule 3: Ensuring data quality

We must keep Personal Data accurate and up to date.

Understanding the Rule

Processing inaccurate information can be harmful to individuals and to Trinity. We must actively encourage individuals to inform Trinity when their Personal Data changes.

Practical Steps

Individuals must be actively encouraged to update their contact details by inviting them, when communication occurs, to notify us of any changes in their Personal Data.

We must ensure that an obligation to keep Personal Data up to date is included in all relevant contracts.

Trinity Examination Service Providers, Representatives, Registered Examination Centres, and Course Providers must update Trinity Online if teacher details change and keep Trinity Online up to date by de-activating teachers that are no longer 'active' i.e. their names are not being displayed on candidates' certificates for that year (de-activated teachers can be re-activated at any time.)

Rule 4: Retaining data

We must keep Personal Data only for as long as is really necessary.

Understanding the Rule

Any Personal Data relating to individuals should only be kept where there is a business or legal need to do so.

Practical Steps

Statutes or regulations may require that certain Personal Data be retained for a specified length of time, and it may also be prudent to keep certain Personal Data for a specific period so that we are able to defend properly any legal claims or manage an on-going business relationship.

Documents (including paper and electronic versions and email) containing Personal Data must not be kept indefinitely and should always be deleted and destroyed once they have become obsolete or when that Personal Data is no longer required. Personal information should not be retained simply on the basis that it might come in useful one day without any clear view of when or why.

Rule 5: Honouring individual's rights

We must always be receptive to any queries, requests or complaints made by individuals in connection with their Personal Data and adhere to our Subject Access Request procedure.

Understanding the Rule

We will reply to queries and complaints in reasonable time and to the extent reasonably possible concerning the processing of Personal Data by Trinity. We consider that the most important of all data protection rights is the ability of individuals to access Personal Data held about them. Individuals are entitled (by making a request to the Trinity) to be supplied with a copy of any Personal Data held about them (including both electronic and paper records).

Other data protection rights include:

- Individuals may object to our use of their Personal Data.

- Individuals may ask us to change the information that we hold on them because they consider our information to be inaccurate or out-of-date.
- Individuals may ask Trinity that no decision taken by us is based solely on the processing of their Personal Data by automatic means for the purpose of evaluating matters relating to them, for example, their creditworthiness.

Practical Steps

Where we receive a request from an individual exercising the right to access their information, we must follow the steps set out in our Subject Access Request Procedure. This procedure is set out in Appendix 6. Our procedure provides a timeline of events to ensure that valid requests are processed in line with applicable legislation.

Where we receive a request from an individual exercising any other data protection right we must notify the Data Protection Officer immediately.

Rule 6: Taking appropriate security measures

We must always adhere to appropriate technical and organisational security measures to protect Personal Data.

Understanding the Rule

Personal information must be kept secure. Technical and organisational security measures are necessary to prevent the unauthorised or unlawful processing or disclosure of Personal Data and the accidental loss, destruction of, or damage to Personal Data.

Practical Steps

- We must monitor the level of security applied to a set of information, taking into account current standards and practices.
- In particular, we must observe the security of information requirements set out in our Information Security Policy
- We must comply with the Data Security Rules set out in Appendix 5.

Rule 7: Using subcontractors

We must ensure that providers of services to us also adopt appropriate and equivalent security measures.

Understanding the Rule

The law expressly requires that, where a provider of a service to Trinity has access to Personal Data of individuals, we impose strict contractual obligations dealing with the security of that information.

Practical Steps

We must always enter into a written contract with any service provider that processes Personal Data on our behalf. All contracts with providers of services should include the standard contractual provisions made available by the Data Protection Officer.

Rule 8: Ensuring adequate protection for overseas transfers

We must never transfer Personal Data outside the EU without ensuring that the recipient provides the right level of protection.

Understanding the Rule

International transfers of Personal Data are not allowed without appropriate steps being taken, such as contractual clauses which will protect the Personal Data being transferred.

Please note that the European Commission has recognised the level of protection provided by data protection laws of Switzerland, Canada, Argentina, Guernsey, Isle of Man, Jersey and the Faeroe Islands as 'adequate'.

Practical Steps

We must not transfer any Personal Data outside the European Economic Area without appropriate steps being taken. Please contact the Data Protection Officer if you are transferring Personal Data to service providers or third parties based overseas.

Rule 9: Sensitive Personal Data: Safeguarding the use of sensitive Personal Data

We must only use sensitive Personal Data if it is absolutely necessary for us to use it.

Understanding the Rule

Sensitive Personal Data is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. This information deserves more stringent protection than other Personal Data, so our standards of care must be higher when dealing with this type of information.

Practical Steps

- We must always assess whether sensitive Personal Data is essential for the proposed use.
- We must only collect sensitive Personal Data when it is absolutely necessary in the context of our business.

Rule 10: Sensitive Personal Data: when to obtain consent

We must only use sensitive Personal Data where we have obtained the individual's explicit consent, unless we have another lawful basis for doing so.

Understanding the Rule

Given the nature of sensitive Personal Data, there are additional conditions in place which we must comply with when we collect and use sensitive Personal Data.

One such condition is that people must expressly agree to the collection and use of such information. This permission to our use of sensitive Personal Data must be genuine and freely given.

Sensitive Personal Data may be collected and used without the explicit consent of an individual where we have another lawful basis to collect and use this type of information.

Practical Steps

- Where application or other forms are used to collect sensitive Personal Data, they must include suitable wording expressing the individual's consent.
- Consent must be demonstrable. Therefore, when it is collected verbally it must be recorded in such a form as to prove that the requisite information was provided to the individual and their responses are able to be verified.
- Where consent is not obtained, we must take steps to ensure that there is another lawful basis under the DPA for the collection and use of such information.

Rule 11: Processing Personal Data of minors

We must be particularly careful when collecting and using Personal Data of minors.

Understanding the Rule

Trinity may process the personal data of minors that are candidates. Minors may not be able to understand the implications of the collection of their personal data. The ICO has issued some guidance documents on this matter according to which data controllers must assess whether the child is mature enough to understand the implications of the collection and processing of their personal data. If the data controller is not sure about this, parent's consent should be obtained.

Practical Steps

Trinity has reviewed this legal requirement and, where possible, relies on obtaining implied consent or, where that is not possible, ensures compliance when processing personal data of candidates that are minors in the context of the test to ensure that they understand the implications of the collection and processing of their personal data. Please contact the Data Protection Officer if you are planning to process personal data of minors in other circumstances e.g. where different rules apply outside the UK.

Rule 12: Legitimising direct marketing

We must always allow customers to opt out of receiving marketing information.

Understanding the Rule

Another important data protection right that individuals have is the right to object to the use of their Personal Data for direct marketing purposes and we must honour all such opt-out requests.

Practical Steps

- We must ensure that the fair processing information notice made available when Personal Data is collected includes the relevant opt-out mechanisms regarding marketing communications. Please see the Data Protection Officer for further information.
- Take all necessary steps to process and record any opt-out requests.

Rule 13: Honouring opt-outs

We must always suppress from marketing initiatives the Personal Data of individuals who have opted out of receiving marketing information.

Understanding the Rule

It is essential that individuals' choices are accurately identified when direct marketing campaigns are carried out. A failure to comply with an individual's opt- out choice (e.g. by sending a mailing to an individual who has previously indicated to us that he or she does not wish to receive mailings) is likely to lead to complaints from the individual and possible scrutiny or enforcement action being taken by the ICO.

Practical Steps

Where we are responsible for a direct marketing campaign, we must take all necessary steps to prevent the sending of marketing materials to individuals who have opted out.

Rule 14: Obtaining consent of email marketing

We must obtain the express consent of individuals to receiving unsolicited commercial communications by email, unless it is legally possible to rely on an "opt-out" approach.

Understanding the Rule

Trinity must obtain the express consent of individuals to receiving unsolicited commercial communications by email.

If the conditions set out below apply, express consent will not be required. Opt-out (i.e. providing the individual the opportunity to object to receiving email marketing) will suffice:

- the email address of the individual has been obtained in the course of a sale or negotiations for a sale of a product or service
- the products or services promoted must be provided by the sender
- the products or services promoted must be similar to those for which the recipient is regarded as a customer

- the opportunity to opt-out of direct marketing must be given when the individual's details were collected
- the opportunity to opt-out of direct marketing must be repeated in every promotional email message

Practical Steps

We should use the language in Schedule 4 as required. The Data Protection Officer may provide further guidance if necessary.

3. COMPLYING WITH THE RULES

3.1 Why is it important that I comply with the Rules?

It is important that everyone within Trinity complies with the Rules, because we are all responsible for data protection compliance. A failure to comply with the rules could expose Trinity to regulatory and/ or legal action which could mean the payment of fines and/or compensation.

3.2 What happens if I breach a Rule?

If you breach a Rule, you should immediately inform your supervisor if you consider the breach to be sufficiently serious. If you are not certain whether the breach is serious, please inform your supervisor in any event. You should always voluntarily tell us of any serious breaches, because we will consider any deliberate cover up or attempts to mislead us about a breach as a serious disciplinary matter.

Additionally, you should note that knowingly or recklessly obtaining or disclosing personal information may be a criminal offence.

3.3 How will compliance be audited?

We will audit compliance with the Rules and we will seek to understand the reason(s) if certain departments or teams are failing to comply with the Rules. Once we have audited the requirements, we will prepare a remediation plan to ensure that the likelihood of the breach recurring is minimised. Should the remediation plan require you to take any actions, we expect you to cooperate fully.

3.3 Who enforces the Act?

The Act is usually enforced by the ICO and the courts. The ICO has powers to serve Information and Enforcement Notices on us, to conduct assessments of our operations and ultimately to fine us. If we fail to respond to the ICO we can be prosecuted in court.

4. TRAINING ON THE RULES

From April 2011, all new joiners, existing employees and contractors will receive training on the Rules. After your initial training, should you feel that you require additional training to ensure compliance with the Rules, please speak to the Data Protection Officer.

5. STATUS OF THE POLICY

This Policy was approved by Trinity's Executive Committee in April 2011.

This Policy will be reviewed every 12 months.

APPENDIX 1

Groups about whom Trinity holds data

Groups about whom Trinity holds data	**Purpose**
Registered Examination Centres/Course Providers	Exam Administration, Contact, Promotion, Payment, Finance Monitoring, Debt Collection
Diploma Candidates (specific to them)	Exam Administration, Statistical Analysis and Reporting
Grade and Diploma Candidates (common to both)	Exam Administration, Statistical Analysis and Reporting
Panel Members	Exam & Staff Administration, Contact, Quality Assurance, Recruitment, Promotion, Payment, Debt Collection, Finance Monitoring
General Contacts	General Contact & Information Gathering
Exam Service Providers	Exam & Staff Administration, Contact, Recruitment, Promotion, Payment, Debt Collection, Finance Monitoring, Statistical Analysis and Reporting Quality Assurance,
Interested Parties	Promotion & Marketing
Regulatory Bodies	Contact
Staff	• administration and maintenance of personnel records; • payment and review of salary and other remuneration and benefits; • provision and administration of benefits (including, if relevant, pension and life assurance); • undertaking of performance appraisals and reviews, including talent review and succession planning; • use during performance, disciplinary, harassment and bullying, and grievance proceedings; • provision of references and information to future employers, and, if necessary, governmental and quasi-governmental bodies for social security and other purposes, the HM Revenue & Customs and the Contributions Agency; • provision of information to future purchasers of the Company or of the business in which individuals work
Suppliers	Contact, Payment
Teachers/Schools	Exam Administration, Contact, Promotion, Quality Assurance
Training Providers	Contact, Quality Assurance, Training
Unsuccessful Applications/ Pending Applications	Contact

APPENDIX 2

Responsibilities of the Data Protection Officer

The nominated contact for the Data Protection Officer is Emma Wells. She can be contacted at emma.wells@trinitycollege.com.

The responsibilities of the Data Protection Officer (which, in many circumstances, will be delegated in whole or in part to a number of persons and spread across various departments) will include:

- Briefing the Director of Operations and IT on data protection compliance
- Reviewing Data Protection and related policies
- Advising staff on Data Protection issues
- Delivering Data Protection induction and training (as appropriate)
- Handling and renewing the notification to the Information Commissioner
- Handling Data Subject access requests and other queries from individuals
- In conjunction with Legal Services, approving contracts with Data Processors
- In conjunction with Legal Services, approving contracts with Data Controllers where Trinity will act as a Data Processor
- Providing guidance on good data protection practice and promoting compliance with this guidance through advising staff on the creation, maintenance, storage and retention of their records which contain Personal Data
- Ensuring compliance with this Policy and the Act.

APPENDIX 3

Data Protection Statement for the Trinity College London website

This relates to where personal data is collected from candidates, teachers, examiners, moderators for the purposes of examination administration, including, but not limited to:

- registration of candidates for examinations e.g. Enrolment Forms;
- management of examinations e.g. Moderation Application Forms.

Where personal data is collected online, this statement does not apply - please refer to our Privacy Policy.

Trinity College London ('Trinity') collects your personal data for the day-to-day administration of our relationship with you and, save where you have agreed, will not use it for any other purpose.

Trinity will not disclose your personal data to any unauthorised person or body, but may disclose your personal data to third party service providers if they need to have access to it in order to render a service to Trinity in relation to the provision of examinations, or to funding and government bodies, if required, and, where appropriate, as required by law. Trinity will not disclose your personal data to other organisations for marketing purposes save to those involved in providing services to Trinity in relation to the provision of examinations.

In the event that any of these third parties are established in a country with data protection legislation that is not equivalent to European data protection laws, Trinity will put measures in place to ensure that your personal data is protected as securely as if it was in Europe.

Where you have consented to receive such information, Trinity may contact you from time to time to provide such information to you about our products, services and events (and those of our third party service providers) and/or to carry out marketing and/or academic surveys and research. If you decide you do not wish to receive these types of communications, please let us know by writing to the address or email address below.

You have the right to request access to the personal data that Trinity College London holds about you. To exercise this right or request further information please write to us at:

Trinity College London
Blue Fin Building
110 Southwark Street
London SE1 OTA, UK

or by sending us an email at privacy@trinitycollege.com

Trinity may update this statement from time to time. The statement governing how Trinity uses your personal data will be the statement in force at the time that your data was collected. Please print a copy for your records.

Date: April 2011

APPENDIX 4

Data Security Rules

1. Security of Data

All staff are responsible for ensuring that any Personal Data which they hold about individuals is kept securely and that they are not disclosed to any unauthorised third party.

All Personal Data should be accessible only to those who need to use it. Personal Data should be kept:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Appropriate security measures must be taken for the deletion or disposal of Personal Data. Manual records should be shredded or disposed of as 'confidential waste'. Hard drives of redundant PCs should be wiped clean before disposal.

2. Disclosure of Personal Data

Trinity must ensure that Personal Data held by Trinity are not disclosed to unauthorised third parties which includes family members, friends, other organisations, government bodies, etc. If in doubt about whether to disclose information in response to an enquiry please contact the Data Protection Officer.

3. General Data Storage

3.1 Hardcopy Data Storage in Trinity's London Office

Hardcopy filing systems in Trinity's London Office must be kept accessible, in order and up to date. Data must be accessible to those that require it for the purpose of exam administration but it should also be kept securely, (e.g. a locked filing cabinet with supervised access). Adequate filing capacity must be provided within each department area. Paper records should be scanned where possible.

Sensitive Data must only be accessible to those with authorisation who should only access the records when they are required. Hardcopy Sensitive Data must never be left on desks or other work areas at any time and must be kept in locked cabinets. Sensitive Data held electronically must be password protected and available to a limited named number of personnel who have access for defined reasons.

3.2 Personal and Sensitive Data Storage

Current Personal and Sensitive Data that is kept by Trinity is held in locked cupboards in Trinity offices. Data is moved regularly to an internal secure storage area where it is held in indexed boxes. Data is eventually moved from this secure area to secure external storage at regular annual intervals.

3.3 Filing Systems External to Trinity's London Office

Trinity Examination Service Providers, Registered Examination Centres, Course Providers and Panel Members must keep records securely. Language Panel Members are required to keep copies of mark sheets for eighteen months and PCA Panel Members are required to keep copies of mark sheets for three months. Equally important is the secure disposal of records once they are no longer active or required for information purposes. Any records must be shredded.

3.4 IT

3.4.1 Trinity Network Servers

Trinity Network servers must be in a secure location and only be accessible to a limited number of named personnel who have access to the network and server passwords.

3.4.2 Trinity Online Data Storage

All examination data held on Trinity Online servers are stored in a secure site accessible to a named group of employees with access rights. Full weekly back-ups are run and incremental daily back-ups of data are taken. Trinity Online is only accessible via a username and password and all users must apply to Trinity Online System Administrator to request a username and password and state for what purposes they will be using Online at the time of application. Users have limited access to the various pages of Trinity Online as a result of the permissions structure that is employed to manage security and access.

APPENDIX 5

Subject Access Request Procedure

Explanatory notes

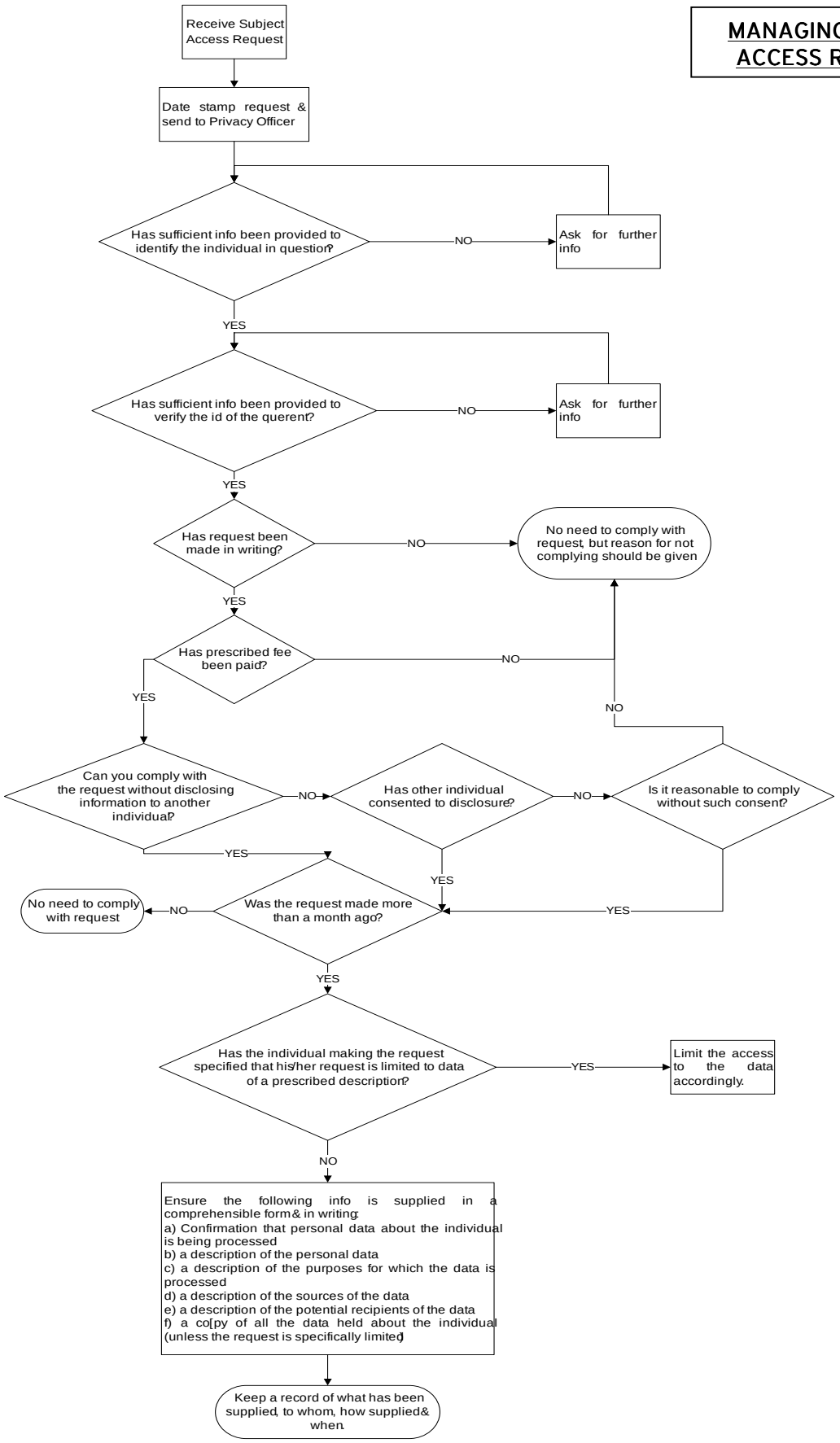
Data controllers are obliged by law to allow individuals to have access to all data held about them. However, such access must only be allowed if certain conditions are met. Follow this checklist each time that individuals ask to be provided with the information that you have about them.

When using the checklist, we suggest that you bear in mind the following points:

- It is easier to deal with access requests if (a) you have appointed a person or team to co-ordinate the provision of information and (b) there are appropriate procedures in place to channel the requests to the appointed co-ordinator.
- Ensure easy access to data held in the organisation and know where it is held.
- A maximum fee of £10 may be charged to provide access (Note: Trinity might be entitled to request higher fees in the event that Trinity's records are considered "educational records" according to Schedule 11 of the Act).
- It may be a good idea to have a standard form of disclosure covering:
  a) Confirmation that personal data about the individual is being processed;
  b) a description of the personal data;
  c) a description of the purposes for which the data is processed;
  d) a description of the sources of the data;
  e) a description of the potential recipients of the data;
  f) a copy of all of the data held about that individual (unless the request is specifically limited).
- If the individual making the request is a child, apply the criteria set out in section 7 above.

TRINITY
COLLEGE LONDON

MANAGING SUBJECT ACCESS REQUESTS



APPENDIX 6

Glossary of Key Terms

Some of the definitions specific to Data Protection are listed below:

Personal Data

Data relating to a living individual who can be identified from that data and other information in possession of the Data Controller. This includes: name, address, telephone number, id number, and also includes expression of opinion about the individual, and of the intentions of the Data Controller in respect of that individual. It does not apply to information about companies and agencies, but does apply to named persons or employees within an organisation.

Sensitive Data

Different from ordinary Personal Data and relates to racial or ethnic origin, political opinions, religious beliefs, health, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular Personal Data, including decisions regarding the purposes for which Personal Data are processed and the way in which the Personal Data are processed. The Data Controller is the legal 'person' responsible for complying with the Act. It will almost always be the organisation, not an individual staff member or volunteer.

Data Subject

The living individual whose personal information is being held or processed by an organisation.

Processing

Any operation related to the organisation, retrieval, disclosure and deletion of data and includes: obtaining and recording data; accessing, amending, adding to, merging, deleting and storing data; retrieval, consultation or use of data; disclosure or otherwise making available of data.

Explicit consent

This is a freely given, specific and informed agreement by a Data Subject to the Processing of Personal Data about her/him. Explicit consent is needed for processing Sensitive Data.

Information Commissioner

The UK Information Commissioner is responsible for implementing and overseeing the Act.

APPENDIX 7

Data Protection – A Brief Overview

Introduction

This overview sets out, in brief, what data protection legislation does and what it means for Trinity College London ('Trinity').

The Data Protection Act 1998 ('the Act') governs the way in which personal data must be handled in the UK and what rights an individual has to know about any personal data held about them.

'Personal data' is essentially data which can be used to identify a living person and can be, or is intended to be, held on computer or in manual records i.e. a 'relevant filing system'.

Any organisation holding and handling personal data must do so in accordance with the following eight overriding principles:

1. That the data is processed fairly and lawfully;
2. That it is obtained and processed for specified, lawful, limited purposes;
3. That it is adequate, relevant and not excessive (regarding the purposes for which it is processed);
4. That it is accurate and, as necessary, kept up-to-date;
5. That it is not kept for longer than necessary for the purposes for which it is kept;
6. That it is processed in accordance with an individual's rights;
7. That it is kept secure (by taking appropriate technical and organisation measures against unauthorised processing and accidental loss, destruction or damage); and
8. That it is not transferred to countries without adequate protection for processing personal data being in place.

There are some exceptions where the Act does not apply e.g. in order to safeguard national security.

Access

A data subject, i.e. an individual who is the subject of personal data, has rights to see the personal data that an organisation holds on him and can make requests about how that information is used and can ask for it to be corrected where it is incorrect. Trinity 'processes' personal data e.g. by organising or using data about candidates, amongst other things, and so is required, by law, to register as a 'data controller'. Trinity, therefore, has certain legal obligations regarding processing personal data.

Consent

In addition, Trinity has other obligations. It has to ensure that when it collects personal data it obtains the data subject's consent to collecting and using the data in the way it proposes - this can be specific or broad consent e.g. for the purpose of administering and providing its examinations. Also, for personal data, the consent need not be in writing, but it must be adequate, with the individual signifying their agreement to its collection and use. Therefore, we can rely on implied consent if appropriate i.e. implied at the point of collecting an individual's details at enrolment. However, for sensitive personal data' i.e. data regarding a person's ethnicity, religious beliefs, health, etc, in particular, where there are special needs, we need to get an individual's explicit consent.

Sharing Data

If Trinity is going to share this data, it must state at the point of collection who it will share it with and for what purposes. Where Trinity is sharing information with third parties who then process the personal data on its behalf, Trinity has to ensure that it has adequate provisions in its contractual relations with that third party to ensure that the third party processes the personal data in accordance with the Act and indemnifies Trinity if it does not.

Compliance

Trinity must, in all instances, comply with the principles listed above. For more details, please see section 3 ('Complying with the Rules') of the Data Protection Policy.

As data subjects can request to see personal data Trinity or related third parties hold about them, it is necessary to be mindful about holding only such data as is required to provide our services; never to hold excessive data; to delete old data and always be wary when emailing or writing anything down about an individual that would constitute personal data, remembering that an individual probably has the right to see it.

Where possible, if there is an issue about a data subject, we suggest not sending emails, but calling to discuss any issues in the first instance.

The Information Commissioner's Office oversees the implementation of the Act. It can require organisations to take various steps regarding data they hold and, ultimately, can fine organisations for breaches of the Act. Its website at www.ico.gov.uk contains very good guidance for anyone who wants to know more about data protection in the UK.