

DATA PROTECTION POLICY

Last Revised June 2008

Contents:

- A. POLICY
- B. GUIDANCE NOTES FOR STAFF

Appendices:

- I. Processing Personal Data
 - *Part 1 – Use of Student Personal Data*
 - *Part 2 – Use of Staff Personal Data*
- II. Retention of Personal Data
- III. Subject Access Request Form

DATA PROTECTION POLICY

Set out below is the Institution's policy and code of practice on data protection, which accords with the Data Protection Act 1988

The code falls into two sections. The first constitutes a statement of general policy, which includes an indication of the Institution's obligations under the Act. The second section provides guidance notes in connection with handling personal data.

A. POLICY

Introduction

1. The Institution needs to process certain information about its employees, students and other individuals, examples of which are set out in paragraph 7 below. In so doing, Trinity Laban must comply with the Data Protection Act 1998 [the Act]. The Act contains eight basic principles, which state that personal data must:

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for longer than is necessary for that purpose
- be processed in accordance with the data subject's rights
- be kept safe from unauthorised access, accidental loss or destruction
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

2. Two of the main features of the Act are that:

- it *places restrictions on what the Institution can do with personal data*; certain conditions, which include obtaining data subject consent, must be met before processing can take place. The term 'processing' covers almost anything that is done to data by reference to individuals and the practical implications of these restrictions are wide-ranging
- it extends the right of *access for staff and students to personal data that relates to them* held in computerised systems to include 'organised' (1) manual filing systems within departments, services and the centre.

(There is *no entitlement to immediate or on-site access* but the Act places a responsibility on the Institution to respond to access requests in good time (2); to this end, all data subject access requests will be handled centrally.

3. *The Institution and all staff or others who process or use any personal information must ensure that the data protection principles and the law under the Act are followed and fully implemented.* In order to facilitate this, Trinity Laban has developed a code of practice on data protection. The references to personal data made within this document apply to all data held on individuals within Trinity Laban, not just students and staff.

Status of the Policy

1. This policy forms part of the formal contract of employment for staff and part of the formal agreement between students and the Institution. Staff, and where appropriate students, must abide by this policy and any failure to comply with the code could result in disciplinary proceedings.
2. Those with 'Visitor' status will also be expected to comply with this policy insofar as they come into contact with personal data through the Institution and in connection with the provision of their own personal data.
3. Staff or students who consider that the policy has not been followed in respect of personal data should raise the matter with the Institution's designated data controller. If the matter is not resolved with the help of the data controller it should be raised under the appropriate grievance or complaints procedures.

What is personal data?

4. Personal data is information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data, which Trinity Laban has or may have in the future. This includes names and addresses, features such as hair and eye colour - which will often be in the form of photographs - student attendance records and marks, ethnic origin, qualifications and experience, details about staff sick and annual leave, dates of birth or marital status. Furthermore, any recorded opinion about or intentions regarding a person are also personal data; and this includes both student progress reports and staff review reports.
5. The Act covers ALL personal data processed by the Institution, irrespective of whether these are held by individual members of staff in their own separate files (including those held outside the Trinity Laban campuses) or in departmental records systems or at the centre of the Institution.
6. The Act distinguishes between *ordinary* personal data such as name, address and telephone number and *sensitive* personal data including information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive data is subject to much stricter conditions. In particular, processing of sensitive data requires explicit consent. However, in most instances consent to process ordinary and sensitive data is obtained routinely by the Institution (see paragraphs 13 - 14 below).

Electronic data

7. Electronically-held data is already covered by the 1984 Act (4). For the avoidance of doubt, this data encompasses not just personal data held on databases but, for example, emails, letters and other documents held electronically.

Manual filing systems

8. The new Act covers 'relevant' manual filing systems, which may have the following characteristics:
 - grouping within a common criteria, even if not physically kept in the same file or drawer
 - structuring by reference to the individual by name, number, student cohort, degree scheme or other mechanism, or by criteria common to individuals, such as sickness, type of job, membership of pension scheme or department
 - and, most pertinently of all, *structuring that allows specific information about the individual to be readily accessible.*
9. In practical terms it is prudent to assume that most manual filing systems fall under the provisions of the Act with effect from October 2001.

Subject Consent

10. In many cases, the Institution can process personal data only with the consent of the individual. In some cases, if the data are sensitive, explicit consent must be obtained. The Institution has a duty, under certain circumstances, to ensure that staff are suitable for the job, and students for the courses offered. On occasion, police checks will be required to verify criminal records. (There are, for example, some jobs or courses which will bring the applicants into contact with children). Where this is relevant to the job, the Institution may also ask for information about particular health circumstances.
11. As noted in paragraph 9 above, in most instances staff - and where appropriate, students - will not need to obtain consent to process from data subjects because such consent is obtained routinely by the Institution. All staff and students are asked to signify their consent to the Institution processing both ordinary and sensitive personal data on application for the purposes of processing that application. Upon student registration or acceptance of an offer of employment, students and staff are asked to give consent to processing a wider range of data. Agreement to the Institution processing this personal data is a condition of acceptance of a student onto any course and a condition of employment for staff; a refusal to provide consent may result in discontinuance of the application. Further information on this point is set out in Appendix I.

Retention of Data

12. It is not in the interest either of data subjects or of the Institution to retain unnecessary or duplicated information. Trinity Laban does, however, retain some data relating to former staff and students - most of which is held in the Trinity Laban Archive - partly in order to comply with statutory requirements but also as a way of maintaining a complete historical record. Nonetheless, it is Trinity Laban policy to discourage the retention of personal data within files for longer than it is needed. Staff are encouraged to work towards the guidelines for the retention of personal data and files forwarded to the Archive should be 'weeded' beforehand in accordance with this guidance.

Access to data

13. Staff, students and others in contact with the Institution will on most occasions have the right to access personal data that is being kept about them either on computer or in 'relevant' manual files. This will normally be provided in the form of copies of the personal data or a report of the data held, depending on the type and format of the original data. Any person who wishes to exercise this right should complete the access request form (see Appendix III) and forward it to the Data Controller. The Institution will levy a charge of £10 on each occasion that access is requested.
14. Where required to do so under the Act, the Institution aims to comply with requests for access to personal information from data subjects as quickly as possible, but will ensure that it is provided within 40 days from the date of the request.

Staff obligations

15. Staff have responsibilities for processing personal data about students (and in some instances, colleagues) but are also data subjects in their own right. In connection with personal data on students and colleagues, all staff must comply with Trinity Laban guidelines on data protection. In connection with their own personal data, all staff should:
 - ensure that any information that they provide to Trinity Laban in connection with their employment is accurate and up to date
 - inform Trinity Laban of any changes for which they are responsible, for example, changes of address (the Institution cannot be held accountable for errors arising from changes about which it has not been informed).

Student obligations

16. Students must ensure that all personal data provided to the Institution are accurate and up to date. They must ensure that any changes, of address, for example, are notified to the Registry department, to their parent department and to other offices as appropriate (the Institution cannot be held accountable for errors arising from changes about which it has not been informed).
17. For the avoidance of doubt it is emphasised that students who come into contact with personal data through the Institution - for the purposes of research or study, in pursuit of an academic qualification and under the direct supervision of a member of staff - will be covered by the Trinity Laban's notification to the Data Protection Commissioner. In such cases, staff must notify students about - and students must abide by - the relevant provisions of the code of practice (and see in particular paragraphs 34-36). The Institution is not responsible for notification of personal data processed by students for their own use.

Data Security

18. All staff (and where appropriate, students) must ensure that:
 - any personal data which they hold are kept securely
 - personal information is not disclosed either orally or in writing, intentionally or otherwise to any unauthorised third party.

19. Staff should note that unauthorised disclosure may be a disciplinary matter, and could be considered gross misconduct in certain cases. (Guidance on authorised disclosure is set out in paragraphs 48-51 below).
20. Additionally, staff must ensure that, where a data processor processes data on Trinity Laban's behalf (a mailing agency, for example) there is a written contract between the parties which specifies that the processor agrees to act on the Institution's instructions and to abide by the provisions of the Act in connection with data security. Further guidance on appropriate terms for such a contract can be obtained from the Head of General Administration.
21. Staff should make reasonable efforts to ensure that all personal information is kept securely but should pay particular attention to the security of sensitive data. All personal data should be accessible only by those who need to use it and sensitive data must be either kept in a lockable room with controlled access, or:
 - kept in a locked filing cabinet, *or*
 - in a locked drawer, *or*
 - if computerised, be password protected, *or*
 - kept only on electronic media which is kept securely.
22. While the security of the Trinity Laban network is the responsibility of the Institution, individuals will need to take appropriate security precautions in respect of day-to-day PC usage. Care must be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. Screens should not be left unattended when personal data is being processed and manual records should not be left where they can be accessed by unauthorised staff. When manual records are no longer required, they should be shredded or bagged and disposed of securely; and the hard drives of redundant PCs should be wiped clean.
23. Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data; and the institutional and personal liability that may accrue from the off-site use of personal data is similarly increased. Staff and students should take particular care when laptop computers or personal machines are used to process personal data at home or in other locations outside the Institution; and staff and students should also be aware that this code of practice and their responsibilities under it apply when data are processed under such circumstances.

Publication of College Information

24. It is Trinity Laban's policy to make as much information public as possible; in particular the following information may be available publicly:
 - lists of staff
 - names and photographs of Board members
 - names and work contact information of staff
 - College e-mail addresses
 - photographs of staff
 - student pass lists.

25. It is of course a condition of employment or registration respectively that staff and students consent to the processing of their personal data (see paragraph 14 above). Nonetheless, it is recognised that there might be occasions when a member of staff or student has good reason for wishing details in certain of these lists or categories to remain confidential or to be restricted to internal access, in which case they should contact one of the designated data controllers. It is understood that this is especially the case in connection with the publication of photographic images of staff, particularly on web pages; all members of staff are advised that such images should not be made publicly accessible without the consent of the individuals concerned.

Monitoring of communications and use of CCTV (5)

26. The Institution must ensure that its resources are not abused or used illegally, for example, for accessing pornographic material on the World Wide Web. In particular, both staff and students have responsibilities for using IT resources in accordance with Trinity Laban regulations. The Institution may from time to time monitor staff and student communications without giving notice; random monitoring of personal computer usage, however, will apply only to publicly accessible computer clusters.

27. For reasons of personal security and to protect Trinity Laban premises and the property of students and staff, close circuit television cameras are in operation in certain locations. Needless to say, there are occasions when, to ensure the effectiveness of this surveillance, the presence of these cameras may not be obvious. Some areas of the Institution may also use webcams, for teaching purposes, for example.

28. In any case:

- any monitoring will be carried out only by a limited number of staff
- personal data obtained during monitoring will be discarded as soon as possible after the investigation is complete
- staff involved in monitoring will maintain confidentiality in respect of personal data

Students or staff who consider that the positioning of a close circuit television camera or use of a webcam is inappropriate should contact the designated data controller (see paragraph 42 below).

World Wide Web and Email

29. The provisions of the Act apply as much to web sites and to email as they do to data processing by any other means; any personal data downloaded from the web, included within a web site, or contained within an email are subject to the same restrictions as information held in manual files or on databases. In particular, authors of web pages should be aware that information posted onto a web page is potentially accessible worldwide (unless access is restricted in some way): the type of data placed onto web pages should reflect this.

Cross-border data flows

30. The new Act places restrictions on the transfer of personal data outside the European Economic Area (EEA)(7), unless the country or territory involved

ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. If, after careful consideration, it is regarded as essential that the transfer of personal data outside the EEA should take place - and if the transfer does not qualify as one of the circumstances when this principle does not apply - the consent of the data subject must be sought. Members of staff should note that: this restriction has particular implications for international research projects and information placed onto web sites (see also paragraph 32 above).

Research data

31. Personal data processed only for research purposes receive certain exemptions where the data are not processed to support measures or decisions with respect to individuals, and where no substantial harm or distress is caused. In essence, such personal data:
 - can be processed for purposes other than that for which they were originally obtained
 - can be held indefinitely
 - are exempt from the data subject right of access where the data is processed for research purposes and the results are anonymised.

32. The Act does not give blanket exemption from all Data Protection Principles for data provided and/or used for research purposes. Most of the Principles apply (notably the requirement to keep data secure); and staff will need to assess the legality of processing on each occasion that data are provided for research purposes (see paragraph 52 below). Furthermore, researchers will need to ensure that:
 - data subjects whose personal data will be used in research are advised as to why the data are being collected and the purposes for which it will be used
 - a suitable mechanism is in place to ensure that data subjects can meaningfully exercise their right to object to the processing of their data on the grounds that it would cause them significant damage or distress
 - **particular care is taken when the processing involves sensitive personal data (see paragraph 9 above for examples) for which stricter conditions apply, including the need to obtain explicit consent for processing.**

33. Finally, those conducting research involving the processing of personal data will doubtless do so in the context of any ethical guidelines or codes of practice particular to their field of study; and it may be necessary to confirm the compatibility of such codes with the Act.

Confidential references

34. Trinity Laban's position at present is to respect the confidentiality of references but under the provisions of Data Protection Act staff must assume that we can neither guarantee confidentiality in respect of references received by the Institution nor expect that those we provide will remain confidential. References drawn up by external bodies before October 2001 should be retained on the understanding that consent to disclose the reference will need to be obtained from the originator if access is sought by the data subject. Advice on the phrasing of a clause suitable for inclusion in written correspondence requesting a reference (making clear the

Institution's inability to guarantee confidentiality) is available from the Head of Human Resources.

Provision of references overseas

35. Explicit consent must always be sought from the data subject where references are provided for organisations located outside the EEA (see paragraph 33 above).

Examination Marks

36. Students will be entitled to information about examination marks. However, this may take longer than other information to provide. (The Institution may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the Institution, but may not withhold marks for these reasons.)
37. Internal and external examiner comments, whether made on the script or in another form that allows them to be held and applied to the original script or to a specific candidate (e.g. an examiner's report) are covered by the Act. A data subject has the right to request that a copy or summary of such data is provided within the stipulated timescale 'in an intelligible form'. This implies that examiner's comments on scripts and assessed work should be capable of being produced for a data subject in a meaningful form and that they should be both intelligible and appropriate.

Conclusion

38. Compliance with the 1998 Act is the responsibility of all members of the Institution. Any breach of the data protection policy may lead to disciplinary action being taken, or access to Trinity Laban facilities being withdrawn, or even a criminal prosecution by third parties. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Institution's designated data controller.

Further information

39. Data protection is a complex area and in addition to the brief guidance notes set out below, further information is available to staff from the Institution's designated data controller:

Jonathan Peel, Director of Operations & Business Enterprise

Email: j.peel@trinitylaban.ac.uk

Further specific guidance for staff follows:

B. GUIDANCE NOTES FOR STAFF

40. In addition to their responsibilities for processing personal data about students (and in some instances, colleagues), staff are also data subjects in their own right. Most staff process personal data about students on a regular basis, when marking registers, or assessments, writing reports or references, as part of a pastoral or academic supervisory role, or in connection with the student administration, including registration, fees, grants, awards, prizes and matters connected with academic appeals and student discipline. Staff frequently also process information about other staff, especially in the context of recruitment and internal procedures, including those for promotion, disciplinary matters and appeals.
41. The Institution will ensure that all students give their consent to processing ordinary and sensitive personal data *via* registration procedures, and that they are notified of the categories of processing as required by the 1998 Act.
42. Consent to process ordinary and sensitive personal data is sought from individual members of staff appointed from February 2001. Staff appointed before this date are deemed to have given their consent.
43. All staff have a duty to make sure that they comply with the data protection principles, which are set out in Trinity Laban's Data Protection Policy. In particular, staff must ensure that records are:
- accurate;
 - up-to-date;
 - fair;
 - kept and disposed of safely, and in accordance with the Institution's policy.
44. All staff, including non-contracted staff, will be responsible for ensuring that data is kept securely.
45. Staff must not disclose personal data to a third party unless:
- the type of data disclosed, and the party or parties to whom it is disclosed, are among those for which consent is sought routinely by the Institution (as set out in the sections on the use of personal data relating to staff and students in Appendix I), *or*
 - if disclosure for such data is not sought routinely, the member of staff or student concerned has otherwise given consent to the disclosure, *or*
 - disclosure is in the best interests of the student or member of staff or a third person, or is otherwise urgent and necessary in the circumstances, or is required in compliance with the law (and see paragraph 49 below).
46. Third party disclosure under the final bullet point of the previous paragraph should occur only in very limited circumstances (for example, if personal data is required urgently where a member of staff or student is injured and unconscious, but in need of medical attention).
47. Where disclosure is requested by the police, *without exception*, the matter should be referred to a member of the Institution's Executive.

48. Where a member of staff is in doubt about how to proceed on third party disclosure, he or she should contact either the relevant departmental advisor or one of the Institution's designated data controller.

Staff Checklist for Processing Data

49. Before processing any personal data, all staff should consider the checklist set out below.
- do you really need to record the information?
 - is the information 'ordinary' or is it 'sensitive' (see paragraph 9 above)?
 - does the Institution have the data subject's consent, i.e. is it included in the sections on the use of personal data relating to staff and students set out in Appendix I
 - are you authorised to collect/store/process the data?
 - unless the data have been obtained from a reliable source, have you checked with the data subject that the data is accurate?
 - are you sure that the data are secure?
 - if you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Access requests

50. The 1998 Act gives individuals the right to access data held about them by the Institution. However, this is not an entitlement to immediate access - the Institution has forty days in which to comply with data subject access requests - and staff should forward all such requests to the Human Resources Manager.
51. The new Act also means that any recorded *opinion about or intentions regarding a person* are also personal data to which a data subject may gain access. This should be borne in mind when written or other records are made (and this includes e-mails and audio recordings, in addition to computer and manual files) and when files are weeded for unnecessary or duplicative material. The following is a useful test to apply to 'doubtful' comments:
- Is this comment fair, accurate and justifiable?
 - If I were to show this to the data subject, would I still be confident that the comment is fair, accurate and justifiable?
52. If the answer to the questions - and in particular the first question - is 'No', then the comment should go unrecorded.
53. Access rights also mean that the confidentiality of references provided either internally or for external bodies can no longer be assumed. Again, this should be borne in mind when references are drawn up and in general terms the information provided in references should:
- confirm the accuracy of or provide factual information
 - differentiate between statements of fact and opinion
 - express only justifiable opinions, based on first-hand experience
 - be fair and accurate
 - avoid ambiguous or coded language.

54. Inappropriate data should neither be recorded nor retained and, needless to say, once a data subject has requested access, data relating to him/her must not be 'weeded'.

Cross-border data flows

55. Staff must take especial care in connection with requests for the transfer of personal data outside the European Economic Area (EEA) (see paragraph 33 above). In particular, staff should not:

- disclose personal data requested by non-EEA governments, agencies and organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas without the specific and informed consent of the data subjects concerned
- disclose personal data requested by non-EEA governments for the purpose of determining liability to attend National Service, without the specific and informed consent of the data subjects concerned.

Further information

Further information and advice is available from the Institution's designated data controller: Jonathan Peel, Director of Operations & Business Enterprise.

Notes

- (1) *Filing systems to be structured in such a way - by alphabetical or subject area, for example - as to allow specific information about individuals to be readily accessible.*
- (2) *Institutions have a maximum of 40 days in which to comply with a request for access by a data subject.*
- (3) *Most of the provisions of the 1998 Act set out in this document already applied to electronically-held data via the 1984 Act. One of the main differences between the two Acts is that, under the 1984 Act, data processed electronically were accessible to data subjects but if such data were converted into manual format and the original electronic format deleted, the right of access was lost. The 1998 Act changes this position - in most instances, manual files will be fully accessible (see paragraphs 11 and 12).*
- (4) *The monitoring of communications and the use of CCTV fall within the ambit of the Act because they invariably involve the processing of personal data in some form.*
- (5) *The European Economic Area consists of the fifteen EU Member States together with Iceland, Liechtenstein and Norway.*
- (6) *It is intended that the primary role of each data protection adviser will be to act as a locus of information about data protection.*

APPENDICES

Appendix I. Processing Personal Data

Introduction

In most instances staff - and where appropriate, students - *will not need to obtain consent to process from data subjects because such consent is obtained routinely by the Institution.*

The data for which consent to process may be considered as having been obtained are set out below. Part I sets out the use of student personal data. Part II sets out the use of staff personal data. Staff - or students - who wish to process personal data not included in these extracts should obtain consent from the data subject(s) first; and should also contact one of the data controllers to alert them to the need to include such data in the periodic review of data for which the Institution routinely obtains consent.

In practice, the day-to-day processing of data will continue as before. An exception to this is research data: in most instances, the College cannot obtain widespread consent in advance of processing and researchers will need to consider individually whether or not they need to obtain consent to process from data subjects.

➤ Part 1 - Use of Student Personal Data

The Institution wishes to make it clear to all students how their personal data (including certain sensitive **(1)** data) will be processed by the Institution. Processing of certain data will for many activities continue after students have left the Institution.

The lists contained below does not preclude the Institution from processing personal data that is included within its registered use under the Data Protection Act or in any other way allowed under the law.

All students agree to the Institution processing their personal data for the following purposes, provided that sensitive personal data may be processed only as set out in clauses 35 - 39 below:

1. Admission, registration and administration of their studies.
2. Academic assessment.
3. Administration of appeals, complaints or grievances.
4. The provision of student accommodation and other support services such as those of the library and career service.
5. The granting of awards.
6. Processing and recovery of accounts and fees.
7. Research and statistical analysis.
8. Production of statistical returns required by certain third party bodies e.g. the Higher Education Statistics Agency.
9. Creation of e-mail addresses, available to those within and outside of the Institution.
10. Completion of references.
11. Direct mailing of publications regarding third party services and Institutional activities and events organised for students.

12. Host mailing of services or career opportunities that the Institution believes may be of interest to students.
13. Administration of employment contracts where the student is employed by the Institution.
14. Administration of the Institution's Alumni relations.
15. Consideration of the award of scholarships.
16. Administration of such codes of practice and policies as apply to students.
17. Use of CCTV to protect Trinity Laban premises and students and staff and their belongings.
18. Production of Student Resource Cards
19. Production of photographs of students for display within the College or on the web.

All students agree that their personal data may be processed and released to third parties for the following purposes:

20. To the Higher Education Statistics Agency, the Funding Council, government departments, and other authorised users for the analysis of student statistics and/or to enable them to carry out their statutory functions as applicable.
21. To the British Council for the administration of pre-arrival events.
22. To The Students' Union for: direct mailing about Union activities, societies and events, administration of Union membership and membership rights, giving of advice on welfare and other issues.
23. To professional and industrial bodies wishing to communicate with students about career opportunities and membership of their body.
24. To direct mail agencies who may assist the Institution in the administration of mailing to students.
25. To the police or other regulatory body where pursuant to the investigation or disclosure of a potential crime.
26. To close family and the emergency services where there is an emergency situation e.g. illness, serious injury to the student or bereavement.
27. To external examiners for the purposes of assessment.
28. To governmental and regulatory bodies for the purpose of gathering census or other information including the assessment of fees.
29. To the Home Office and other international and national governmental and regulatory bodies in connection with the assessment of students status.
30. To other bodies involved in the delivery of the course or programme e.g. affiliated colleges, for the purpose of statistical analysis, assessment, administration and award; and exchange institutions, including those outside the EEA.
31. To professional bodies where registration with that body is related to or a requirement of the student's studies.
32. Trinity Laban's Alumni branch offices/representatives within and outside of the UK for dissemination of information in connection with activities and events for former students.
33. To any third party accessing Trinity Laban's e-mail directory of student e-mail addresses.
34. To any third party wishing to access a catalogue within the Institution's libraries containing reference to student work.

35. To third parties accessing information about student awards - ranged by department - which is available in the public domain.

All students agree to the College processing their sensitive personal data (data about racial or ethnic origin, physical or mental health, commission or alleged commission of criminal offences) for the following purposes and for release to the following third parties:

36. To the Higher Education Statistics Agency, the Funding Council, government departments and other authorised users for the analysis of student statistics and/or to enable them to carry out their statutory functions as applicable.
37. To professional bodies where registration with that body is related to or a requirement of the student's studies.
38. To other bodies involved in the delivery of the course or programme e.g. affiliated colleges, for the purpose of statistical analysis and programme administration.
39. Unless otherwise agreed with the student, within the Institution only, for the assessment and provision of services to disabled students and for the admission and administration of student programmes.
40. For admission to and the administration of student programmes.
41. Where required, to the police or other agencies in connection with particular programmes of study or prior to certain placements.

Provision of Personal Data to a Third Party

Except as otherwise provided for in the 'Use of Student Personal Data' statement set out above, or unless written authorisation has been provided by the student concerned, the Institution does not release information that could constitute personal data to any third party (including parents, relatives and friends).

➤ Part II - Use of Staff Personal Data

The Institution wishes to make it clear to all members of staff and other workers how the Institution will process their personal data (including certain sensitive **(1)** data). In essence, in order to function normally, the College needs to process 'ordinary' and 'sensitive' personal data for employment-related purposes. Processing of certain data will for some activities continue after individuals have left the service of the Institution.

The list shown below does not preclude the Institution from processing personal data that is included within its registered use under the Data Protection Act or in any other way allowed under the law.

All members of staff and other workers agree to the Institution processing their personal data for the following purposes:

1. Payment of salary, pension, sickness benefit or other payments due under the contract of employment.
2. Monitoring absence or sickness under an absence control or capability policy.
3. Training and development purposes.
4. Management planning.
5. Providing and obtaining references and consultation with external agencies, including police checks where necessary for the purposes of employment.

6. To the police or other regulatory body where pursuant to the investigation or disclosure of a particular crime.
 7. Promotion and salary progression exercises.
 8. Negotiations with trade unions or other staff representatives
 9. Curriculum planning and organisation.
 10. Timetable organisation.
 11. Administration of Trinity Laban's codes of practice and policies.
 12. Compliance with the Disability Discrimination Act.
 13. Compliance with any statutory or legal requirement to provide information about staff or other workers including, for example, statistical returns to external bodies and staff membership lists to Unions.
 14. Administration of Trinity Laban's disciplinary and grievance procedures.
 15. Direct mailing for third party services reasonably concerned with employment-related matters or staff benefits.
 16. Production of published staff lists including telephone and e-mail directories for both internal and external use.
 17. Production of Staff Resource Cards.
 18. Production of photographs of staff for display within the College or on the web (but see also paragraph 29 of the Trinity Laban's code of practice on data protection).
 19. Development of staff research profiles by associated Trinity Laban companies.
 20. Monitoring the use of Trinity Laban resources.
 21. Use of CCTV to protect Trinity Laban premises and staff and students and their belongings.
 22. In relation to the provision of academic services and other services (for example, car parking).
 23. In relationship to membership of Institution and staff clubs, societies and similar organisations.
 24. To close family and emergency services in the event of an emergency, for example, illness, serious injury to the member of staff or bereavement.
 25. Production of statistical returns required by certain third party bodies e.g. the Higher Education Statistics Agency.
- (1) Sensitive personal data includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions.**
-

Appendix II. Retention of Personal Data

UNDER REVIEW

Document and Data Retention Guidelines

1. **Notes**
2. **Finance Office**
3. **Registry Office**
4. **Human Resources Office**
5. **Archiving**

1. Notes

- (a) The Executive of the institution has agreed the retention periods identified in this section. Members of each office listed in this section must ensure that these guidelines are followed in arranging for the storage, retention or destruction of documents belonging to the area under their control.
- (b) Where a retention period of twelve months is specified, the documents must be retained until the completion of the final audit for the year to which they relate.
- (c) Where a retention period of one year is specified, the records must be retained for 1 year after the completion of the final audit for the year to which they relate. Similarly with 2 years, 6 years etc.
- (d) Items marked # are to be shredded at the expiry of the retention period.
- (e) Any records not required on a day to day basis should be stored in the College's archives.
- (f) The line manager for each section is responsible for the good order of his or her part of the archive and should ensure that all documents are clearly labelled while in store and marked either for destruction, with a date, if appropriate (e.g. mm/yy) or an infinity symbol (∞) if on permanent retention.
- (g) An annual review of documents in store should take place at a convenient time after completion of the annual audit so that documents no longer required can be destroyed.
- (h) The following guide is to be used as a basis to minimum retention periods only. Records may be retained for longer if necessary.

2. Finance Office

<u>NARRATIVE</u>	<u>RETENTION PERIOD</u>
Annual Ledger/Transaction Reports	Permanent
Final Accounts	Permanent
Year End Tuition Fees Summaries	20 years
Suppliers Invoices/payment vouchers	6 years
Remittance Advices	6 years
Petty Cash Vouchers	6 years
Journal Reports	6 years

TRINITY LABAN CONSERVATOIRE OF MUSIC & DANCE

Cash Book Payments Sheets	6 years
Debtor Invoice Copies	6 years
Bank Reconciliation Statements	6 years
Bank Statements	6 years
Cash Received Summaries/Pay in slips	6 years
Scholarships and Prizes	6 years
Student Loans Documentation	3 years
Hardship Awards	3 years
Access Documentation	3 years
Cancelled Cheques	3 years

3. Registry Office

<u>NARRATIVE</u>	<u>RETENTION PERIOD</u>
Student Records, including academic achievements and conduct.	At least 6 years from the date that the student leaves the College,
	At least 10 years for personal and academic references

(to be completed)

4. Human Resources Office

The following guide is to be used as a basis to minimum retention periods only. Records may be retained for longer if required.

<u>NARRATIVE</u>	<u>RETENTION PERIOD</u>
Personal Files and incl' training records/contracts	6 years from the end of employment
Application forms/interview notes	1 year from date of last interview
Pay Rates Printouts	Permanent
Income Tax and NIC returns /Payroll Reports/Summaries	At least three years after the end of the financial year to which they relate
Pay Journals Reports	At least three years after the end of the financial year to which they relate
Pension Files/Reports	25 years
Teacher's Pay Claims/Summaries	At least three years after the end of the financial year to which they relate
Cost Analyses	At least three years after the end of the financial year to which they relate
Wage Slips	At least three years after the end of the financial year to which they relate
Fee Contracts for external examiners etc.	At least three years after the end of the financial year to which they relate
Year End A/c Reconciliations/Documents	At least three years after the end of the financial year to which they relate
Creditors payment summaries	At least three years after the end of the financial year to which they relate
PAYE Code Adjustments	At least three years after the end of the financial year to which they relate
Budget Analyses	At least three years after the end of the financial year to which they relate

Student Instrument Loan Documents	At least three years after the end of the financial year to which they relate
P46 / P38s Forms	At least three years after the end of the financial year to which they relate
Bank Reference Statements	At least three years after the end of the financial year to which they relate
Staff Sick & Maternity Leave Records	At least three years after the end of the financial year to which they relate
Travel Loan Documents	At least three years after the end of the financial year to which they relate
Interim Payments	2 years
Copy of Job Adverts	1 year
Staff Annual Leave Records	1 year
Job Applications Rcv'd and rejected	1 year
Health Records	During Employment
Payroll Time Sheets & input documents	3 Years

5. Archiving

- (a) The archiving system has been designed by the Facilities Management Department (FMD) to ensure uniformity throughout the institution.
- (b) The FMD will control all archiving, ensuring that all faculties and departments archive using a standard format, the correct boxes and labelling. No boxes will be accepted into store without the label showing all relevant information.
- (c) Archiving should be carried out on an annual basis and can take place at various times during the year. Ideally, most general documents/files should be archived at the end of each academic year.
- (d) Certain departments (e.g. Finance & Human Resources) may find it more convenient to archive after the completion of the tax year-end and the financial year-end.
- (e) Destruction of boxes will take place at the beginning of the month following the destruction date marked on the box label.
- (f) To send a box to archiving requires some simple steps. Following these correctly will enable your box to be archived in the correct section, make for easy identification and retrieval and remain in good condition during its time in storage.

STEP 1

Order a box of adequate size from the Estates & Facilities department and assemble as per the instructions.

STEP 2

Place documents/files inside using either cardboard covers or any other suitable method of separation and protection. Boxes should not be overloaded and always kept at a manageable weight.

STEP 3

The contents of the box should be listed and a reference number added (relevant to the faculty and department and agreed by the line manager) on the label template (copies available from House Services). One copy should be photocopied and one taped or glued

to the inside of the box lid. The original copy should be glued to the front of the box. (Tape should not be used as this dries out and, after time, the label will fall off)

STEP 4

The contents should be listed on a department list and filed in the faculty/department archive file.

If unsure as to when the boxes should be marked for destruction, the line manager will be able to advise.

Last updated April 2007

Appendix III.

Subject Access Request Form

1. Details of the person requesting the information:

Full name:

Address:

.....

.....

Telephone Number:Email:

2. If you are not the Data Subject, you must supply the details of the Data Subject, together with their written authority to act on their behalf.

Details of the Data Subject (if different from 1. above)

.....

.....

3. Please describe any specific document(s) you wish to see below, e.g. particular report or specific departmental file:

.....

.....

If you would like a more general search, indicate below any sections/departments that you have been in contact with which you would like to be searched for relevant data:

.....

.....

Please note that the institution reserves the right to obscure or suppress information which may relate to other third parties (under the terms of Section 7 of the Data Protection Act 1998)

Declaration

I certify that the information given on this application is true. I understand that a fee of £10.00 is payable, and this is enclosed, together with relevant documents:

Signed _____

Dated _____

Documents which must accompany this application are:

- i) Evidence of your identity
- ii) If you are not the Data Subject - evidence of the Data Subject's consent to disclose information
- iii) £10 fee (cheques to be made payable to Trinity Laban)
- iv) Stamped addressed envelope for return of proof of identity/authority documents, where appropriate

Please return this form to the Data Controller:

**Mr. Jonathan Peel
Director of Operations & Business Enterprise
Trinity Laban Conservatoire of Music and Dance
King Charles Court
Old Royal Naval College
Greenwich
LONDON
SE10 9JF**