DATA PROTECTION POLICY

Originator: **Dave Russell**
Date: **January 2012**
Approved by: **SMT**
Type: **Policy**

Revised: **March 2015**

CONTENTS

1 INTRODUCTION

1.1 Leeds College of Art, hereafter known as the College, needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- 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.

1.2 The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed the Data Protection Policy.

2. STATUS OF THE POLICY

2.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2.2 Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

3. NOTIFICATION OF DATA HELD AND PROCESSED

3.1 All staff, students and other users are entitled to know:

- What information the College holds and processes about them and why.

- How to gain access to it.
- How to keep it up to date.
- What the College is doing to comply with its obligations under the 1998 Act.

3.2 The College will therefore provide all staff and students and other relevant users with a standard form of notification. This will state all the types of data the College holds and processes about them, and the reasons for which it is processed.

4. RESPONSIBILITIES OF STAFF

4.1 All staff are responsible for checking that any information that they provide to the College in connection with their employment is accurate and up to date and amended accordingly.

4.2 If and when, as part of their responsibilities or as part of academic research, staff collect information about others (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff (see appendix A).

5. DATA SECURITY

5.1 All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party,

5.2 Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out in 5.3 to 5.7 inclusive below will usually be a disciplinary matter, and may be considered gross misconduct in some cases. Guidance on disclosure and sharing of personal information relating to students can be found in Appendix D.

5.3 Personal information should be;

- kept in a locked filing cabinet; or
- in a locked drawer; or

Personal data that is computerised should be stored securely following the College's Computer Security Policy respecting requirement regarding password and encryption conventions.

5.4 Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

5.5 Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or

appropriate, the agreement of the relevant Data Controller must be obtained and all the security guidelines given in this document and in the College's Computer Security Policy must be followed.

5.6 Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:
- Suitable backups of the data exist
- Sensitive data is appropriately encrypted
- Sensitive data is not copied onto portable storage devices without first consulting a Data Controller with regard to appropriate encryption and protection measures.
- Electronic devices such as laptops, mobile devices and computer media (USB devices, CD's etc) that contain sensitive data are not left unattended when offsite.

5.7 Cloud services should not be used for the transport or storage of any non-anonymised or unencrypted personal data, guidance on the use of Cloud services for other data can be found in the College's Computer Security Policy.

5.8 For some information the risks of failure to provide adequate security may be so high that it should never be taken home. This might include payroll information, addresses of students and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of the Principal.

6. STUDENT OBLIGATIONS

6.1 Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc are notified to the Course Administrator.

6.2 Students may also, from time to time, process personal data as part of legitimate academic research. In any such event this processing should be carried out only in accordance with this policy and the College's Ethics Policy.

7. RIGHTS TO ACCESS INFORMATION

7.1 Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in central files. Any person who wishes to exercise this right should complete the college "Request form for access to data" and return it to the Academic Registrar or Head of HR as appropriate.

7.2 In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached. The College will make a charge of £l0 on each occasion that access is requested, although the College has discretion to waive this. The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

8. PUBLICATION OF COLLEGE INFORMATION

8.1 Information that is already in the public domain is exempt from the 1998 Act. It is the College policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names and contacts of College governors
- List of key staff

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact a designated data controller.

9. SUBJECT CONSENT

9.1 In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent, must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

9.2 Some jobs or courses will bring the applicants into contact with children, including young people under the age of 18. The College has a duty under the Children Act and other enactments to ensure that staffs are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

9.3 The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

9.4 Therefore, all prospective staff and students will be asked to sign a 'consent to process' form, regarding particular types of information when an offer of employment is made or a student enrolment takes place. A refusal to sign such a form can result in the offer being withdrawn.

10. PROCESSING SENSITIVE INFORMATION

10.1 Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as those for sick pay or equality and diversity. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, Staff and students will be asked to give express consent for the College to do this. Offers of employment or student places may be withdrawn if an individual refuses to consent to this without good reason. More information about this is available from designated data controllers.

11 THE DATA CONTROLLER AND THE DESIGNATED DATA CONTROLLERS

11.1 The College as a body corporate is the data controller under the Act, and the board is therefore ultimately responsible for implementation. However, there are designated data controllers who deal with day to day matters.

This College has designated 5 data controllers. They are;

Sharon Bailey	-	Director of Finance
Graham Curling	-	Head of Human Resources
Dave Russell	-	Director of Studies, Progression and Student Support
Simon Thorpe	-	Director of Studies, Professional and External Engagement
Randall Whittaker	-	Director of Studies, Higher Education Enhancement and Research

12. EXAMINATION MARKS

12.1 Students will be entitled to aggregated information about their marks for both coursework and examinations. However, this may take longer than other information to provide.

13. RETENTION OF DATA

13.1 The College will keep some forms of information for longer than others. Because of storage problems, information cannot be kept indefinitely. In general information about students and staff will be kept for a maximum of six years after they leave the College. The College Record Management Policy and Record Retention Schedule provide further detail on this and should be read alongside this policy.

14. CONCLUSION

14.1 Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated data controller.

APPENDIX A

Staff Guidelines for Data Protection

All staff will process data about students on a regular basis, when marking registers, or College work, writing reports or references, or as part of a pastoral or academic supervisory rote. The College will ensure through registration procedures. that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address,
- Details about class attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline,

Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the students consent. If staff need to record this information, they should use the College standard form.

E.g. Recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the College 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 College policy.

The College will designate staff in each area as 'authorised staff', These staff are the only staff authorised to hold or process data that is:

- not standard data; or
- sensitive data,

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is

- necessary;
- in the best interests of the student or staff member, or a third person, or the College; AND
- he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances .

This should only happen in very limited circumstances e.g. a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's witness.

Authorised staff will be responsible for ensuring that all data is kept securely.

Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the College policy.

Staff shall not disclose third party personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with College policy.
Before processing any personal data, all staff should consider the following checklist.

Staff checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the student been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is 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?
- Have you reported the fact of data collection to the authorised person within the required time?

APPENDIX B

LEEDS COLLEGE OF ART

Request Form for Access to Data According to the Data Protection Act 1998

I, […….name] wish to have access to Data that the College has about me in the following categories:

- Academic marks or course work details
- Academic or employment references
- Disciplinary records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc.
- Other information

(Please tick as appropriate]

I understand that I will have to pay a fee of £10 to contribute to photocopying and other administration costs.

Signed:

Dated:

APPENDIX C

The Data Protection Act 1998

Glossary

Data - Any information which will be processed or used on or by a computerised system. This can be written, taped, photographic or other information

Personal Data Information about a living person. This information is protected by The Act

Data Subject - The person whom the data is about

Data Controller - The person or Organisation responsible for ensuring that the requirements of the Data Protection Act are complied with

Designated Data Controller - Individual appointed by the College to carry out the day to day duties of the Data Controller

Data Processor - Any person other than a person employed by the Educational institution, who processes any data on behalf of the Organisation. An external payroll provider will be an example

Processing - Accessing, altering, adding to, changing, disclosing or merging any data will be processing for the purpose of the 1998 Act

Sensitive Data - Information about a person's religion or creed, gender, trade union membership, political beliefs, sex life or sexuality, health or criminal record

Relevant Filing System - Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible

The Data Protection principles - the underlying principles of the Act that determine what data can be collected, processed and stored. A failure to abide by the principles will be a breach of the 1998 Act.

The Data Protection Commissioner - Person Appointed by the government to administer the provisions of the 1998 Act including notification and to provide guidance and assistance to organisations and individuals

The Data Protection Tribunal - The tribunal established to deal specifically with matters of enforcement under the Data Protection Act

Notification - The process of informing the Commissioner that an Organisation or an individual will be processing personal data other than for private use. This replaces registration under the 1984 Act.

Subject Consent - Before processing personal data, the College must have the agreement of the individual to do so. In the case of sensitive data, this must be specific consent, but in other cases, it can be more general

APPENDIX D

Disclosure and Sharing of Personal Information Relating to Students

Prospective, current students and alumni need to have confidence that the College will protect their privacy and personal data. It is important for there to be clear principles in place with regard to how personal information will be handled. This guidance outlines the process to be followed by all staff at the College.

1. **What the College means by Confidentiality**

1.1 Personal information is defined as: information that relates to an individual, from which they can be identified. Staff to whom the student has made a disclosure should handle personal information carefully, in accordance with the College's Data Protection Policy. Information about matters of health, relationships, political affiliations, criminal record, religion or ethnicity is sensitive and must be respected.

1.2 Personal information about a student will only be shared with other staff in the College, or with an external agency with the consent of the individual. Consent should be in writing and held with the student's record within the programme administration team. Personal information will only be shared within the College on a 'need to know' basis and students should be informed of to whom any personal information is being disclosed.

1.3 The College acknowledges that occasions may arise where individual staff need to breach confidentiality. Such circumstances include:

- where there is an immediate and serious threat to the personal safety of those concerned;
- where there is an immediate and serious threat to the safety of others;
- where there is a legal requirement to disclose that information (e.g. a crime has been committed, or it is covered by health and safety legislation);
- to prevent a criminal act, especially where others may be endangered, for example an act of terrorism;
- where professional fitness to practice may be compromised.

1.4 Further exceptions may apply to students aged under 18 years, who are not legally classed as adults. For example when there are concerns about a student's wellbeing, and where in certain circumstances it may be necessary to disclose information to parents, guardians or statutory authorities, e.g. Social Services, Police, etc.

2. Seeking consent and sharing information

2.1 If a student chooses to withhold consent for information to be shared, it should be made clear that this may limit the kinds of support that are open to them. In exceptional circumstances, it may still be necessary to disclose the information to others, whilst also making it clear that such disclosure would be on a need-to-know basis only, emphasising strict confidentiality in relation to any other third party.

2.2 Absolute assurances of confidentiality to those who may wish to talk about personal issues should be avoided, it is more appropriate to outline the limits to confidentiality. It may be

necessary to say that information may be shared with discretion with others who need to know it, if this is in the best interests of the individual and the College.

3. Communicating with external enquirers

3.1 When communicating with parents, spouses, other relatives, partners or guardians, the guidance note below should be followed.

3.2 UCAS applicants are asked whether they wish a parent or representative to be authorised to discuss their application with UCAS. This type of agreement is not transferable to the College without the student's consent.

3.3 Statutory authorities (e.g. Police, Children and Social Services) may have a legitimate reason for requesting information, e.g. concern about the safety of a person, a criminal investigation, etc. Additionally, a request for information may come from the Independent Safeguarding Authority. Any such request must be made in accordance with the correct processes under Data Protection legislation.

3.4 An enquirer may claim to know that a student is registered as being a student of the College. This information should be neither confirmed nor denied, stating this is our policy.

4. Disclosing information to the police

4.1 The College is committed to acting in a lawful and ethical manner, and expects its students to act similarly. The police must provide an **information request form** (under the Data Protection Act 1998 section 29(3)) in respect of all enquiries.

Where the Police advise the college that they wish to receive information in respect of a student they believe has committed an offence the college will provide them with the following personal information using the information request form:

- Personal details (name, address, contact number)
- Course details (course of study and mode of attendance)
- Current status details (whether a student is active or withdrawn)
- Timetable/rooming information will not be provided.

Where the police advise the college that they wish to receive information in respect of a student they believe witnessed an offence, or may assist in some other way, the college will confirm whether or not the individual is a current student, but will not normally provide further information. The college will offer to contact the student direct and request that they speak to the police. If the student so wishes, the student may ask to be accompanied by a member of staff if the meeting takes place on college premises during normal working hours.

GUIDANCE NOTE

Guidance on Communicating with the Parents, Guardians, Spouses, Partners or Relatives of Students (including applicants and former students).

General principles

This guidance is intended to offer assistance to staff dealing with the parents, spouses, relatives or guardians of applicants, students and former students. (The words 'parent' and 'student' are used generically to cover these categories).

Students who are over 18 are adults and have the same legal rights as any other adult regarding confidentiality. In particular, they are protected by the Data Protection act. Personal data about a student (which could include the status of their application, confirmation that they are studying here, where they live and how their studies are progressing) should not be disclosed to anyone else without the express consent of the student.

Particular care should be taken over information about a student's political or religious beliefs, their physical or mental health, their sexual life and any criminal issues. In law this constitutes 'sensitive personal data' for which have specific consent to disclose must be given. Disclosure without consent is a breach of the Data Protection Act.

Parents have no legal right to information about their offspring while at College although they would be contacted as next of kin in the event of an emergency or real concern about the welfare of their son or daughter (e.g. if they go missing). If a parent contacts the College by telephone, email or in person, without the student present, staff should politely decline to discuss the student's affairs with them without the student's consent.

A student who is under the age of 18 may also refuse to give consent to the College to talk to their parents, and should be treated in the same way as over 18s. In exceptional circumstances (e.g. a serious and imminent risk to the welfare of the student) it may be appropriate to contact parents.

In the event that enquirers are particularly persistent or refuse to recognise confidentiality arrangements they should be referred to the Academic Registrar.

Giving consent

Consent should only be sought in very serious circumstances; wherever possible the College should encourage autonomy and resilience for students. However, general information about college process can be given as they are publicly available. Consent should be in writing, using a password agreed with the student, and should specify the particular issues that the student is happy for us to discuss e.g. a complaint, or accommodation issues, or ill health. Passwords should be kept centrally in the Special drive, so that they can be accessed by staff who have authorisation to communicate about the issues specified.

If the student asks about the form of wording the suggested format is:

'I consent to my mother/father/spouse/guardian/other [name] contacting the College on my behalf about the following issue (s) using the password xxx agreed by me on [date]'

[Give details of issue]

Signed…..

Dated……

Email authorisation can be accepted where this is sent from one of the following:

- The email address given at the point of application (for applicants).
- The Student's College email address (for those currently registered).

The exception to this is where a parent is present with the student, and the student confirms verbally that they are happy for an issue to be discussed with or in front of their parent. The staff member speaking to them should make a note that verbal consent has been given. This applies to face to face and telephone communication. For additional security asking for the student's ID number will clarify that the person being spoken to is the student. It is also good practise to ask if the parent has a speaker phone so that the student can listen in.

The only exception to the requirement for written consent may be:

- For a student with a disability, where it may be a 'reasonable adjustment' to agree to communicate with the parent, if the student has particular difficulties with communication. Even then, the student must have given their consent.

- In an emergency, or if the student is too unwell to speak to The College or provide consent.

It is appropriate, and often very helpful, to outline the general process and relevant context for a parent, without disclosing specifically the situation of the individual. This could include an explanation of application processes, or information about how a student should raise a complaint or general matter of concern. This may enable the parent to guide the student towards more effective resolution of any problems or personal difficulties.