CLEVELAND COLLEGE OF ART & DESIGN

Title	Data Protection Policy		
Version number:	1.0		
Author:	Stuart Slorach, Vice Principal – Resources		
Consultation taken place with:	MIS Manager	Dates:	March 2015
Approved by:	Principalship	Date:	March 2015
Date to be reviewed:	March 2018		

The policy or procedure will be reviewed by the date shown on the front cover sheet, or sooner if a change in legislation, best practice, or other circumstances indicate that this is necessary. If, for whatever reason, the policy or procedure is not reviewed by the date shown, the policy or procedure shall stay in force until formally reviewed.

Introduction

1) The College is required to retain certain information about its employees, learners and other users in order to facilitate the monitoring of performance, achievements, and health and safety. 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 and disposed of 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 to be kept for longer than is necessary for that purpose;
    - Be processed in accordance with the data subject's rights;
    - Be 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) 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.

Status of the Policy

3) This policy does not form part of the formal staff contract of employment nor of the student contract with the College, but it is a condition of both contracts that College regulations and policies must be adhered to. A failure to follow the policy may result in disciplinary proceedings.

4) Any members of staff or learners who consider that the policy has not been followed in respect of personal data about themselves or about other data subjects should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal complaint or grievance.

Definitions

5) None required

Notification of data held and processed

6) All staff, learners and other data subjects 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.

7) If and when, as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to other academic institutions and details of personal circumstances), they must comply with the guidelines for staff.

Responsibilities of Staff

8) All staff are responsible for ensuring that:

    - Checking that information they provide to the College in connection with their employment is accurate and up to date.
    - Informing the College of changes to information which they have provided, e.g. change of address.
    - Checking the information that the College will send to them from time to time, which gives details of information kept and processed about them.
    - Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

Data Security

9) 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 a third party.

10) Staff should note that unauthorised disclosure and / or failure to adhere to the requirements set out in 11 to 16 inclusive below will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

11) Personal information should be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected; or
- When kept or in transit on portable media the files themselves must be password protected.

12) 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.

Student Obligations

13) 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 relevant administrators.

14) Students who use the College computer facilities may, from time to time, process personal data. If they do they must obtain the prior permission of their course or programme tutor.

Rights to Access Information

15) Staff, students and other users of the College have the right of access to any personal data that are being kept about them either on computer or in certain other files. Any person who wishes to exercise this right should complete the College "Access to Information" form and give it to the designated data controller or, in the case of a student, to her/his course tutor or lecturer. Forms are available from the main office.

16) The College will normally make a charge of £10 on each occasion that access is granted, although it has discretion to waive this charge for good reason at the discretion of the Data Controller.

17) The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 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.

Publication of College Information

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

- Names of College governors;
- List of key staff;

- Annual Report and accounts.

The College's internal phone list and student room list will not be public documents.

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

Subject Consent

19) 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.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Childrens Act and other enactment's to ensure that staff 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.

The College will also ask for information about particular health needs, such as allergies to particular forms or 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.

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 or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Examination Marks

20) Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold results, certificates, accreditation or references in the event that the fees or other debts have not been paid, or all books and equipment returned to the College.

Processing Sensitive Data

21) 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 the sick pay policy or equal opportunities policy. 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 course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the HR Department.

The Data Controller and the Designated Data Controllers

22) The College as a corporate body is the data controller under the Act, and the Governing body is therefore ultimately responsible for implementation. However, the designated data controllers who will deal with day to day matters are:

- Stuart Slorach — Vice Principal – Resources
- Charly Butler — MIS Manager
- Amy Clark — Human Resources Manager
- Bill Goodwin — IT Manager
- Clare Moore — Financial Controller

Retention of Data

23) The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general information about students will be kept for a maximum of 10 years after they leave the College. This will include:

- name and address (including e-mail address);
- academic achievements, including marks for coursework; and
- copies of any reference written.

All other information, including any information about health, race or disciplinary matters will be destroyed within 6 years of the course ending and the student leaving the College.

The College will need to keep information about staff for longer periods of time. In general, all information will be kept for 6 years after a member of staff leaves. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Conclusion

24) 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 co-ordinator

Equality Statement

25) This policy will be implemented in line with the principles of the college's commitment to equality and diversity which is: Cleveland College of Art and Design is committed to the principles of equality and diversity and aims to ensure that all employees and college users are treated fairly and equally regardless of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation.

Related Documentation

26) None