MORLEY COLLEGE LONDON

Information and Data Protection Policy

POLICY OWNER: Clerk to the Governing Body and Company Secretary
APPROVAL: Governing Body
APPROVED: 26 March 2018
NEXT REVIEW: 31 March 2019

Equality Analysis Screening

Equality analysis is a way of considering the effects on different groups protected from discrimination by the equality act. Consider if there are any risks within this policy that will adversely affect a particular group or a variety of groups. Are there any changes that need to be made to the policy its self or additional actions that need to be made to mitigate the risks? The protected characteristics are:

Race
Gender
Disability
Age
Sexual Orientation
Gender reassignment
Religion and Belief
Maternity and Pregnancy
Marriage and Civil Partnership

Risks identified:

None

Evidence used (data, consultation):

Information Commissioner's Office: *Guide to Data Protection*
Information Commissioner's Office: *Guide to the General Data Protection Regulation (GDPR)*
Information Commissioner's Office: *Preparing for the General Data Protection Regulation*
Association of Colleges guidance note: *Colleges and the General Data Protection Regulations*

Consultation and further consideration through the College GDPR Task and Finish Group

Does this policy need a further action before it can be approved?
(changes made to policy or further equality analysis needed)

No

INFORMATION AND DATA PROTECTION POLICY

1. INTRODUCTION AND PURPOSE

Morley College London needs to collect and maintain certain information about its employees, students and other users of its services to allow it to monitor, for example, performance, achievements, and health and safety. It is also necessary to process information so that governors, employees and students can be recruited, employees paid, courses organised, external funding secured and legal obligations to funding bodies and government complied with. Accordingly, data may be collected not only from and about actual governors, employees, students and service users, but also from and about a wide range of individuals having or contemplating dealings with the College, including prospective governors, employees and students, Friends of Morley, past and potential future donors, individuals involved in fund-raising and other individual stakeholders.

In order to ensure that information is collected and used fairly, stored safely and not disclosed to any other person unlawfully and that employees or others who process or use any personal information ensure that they follow the Data Protection Principles set out below, the College has adopted this Information and Data Protection Policy

2. MORLEY COLLEGE IN CONTEXT

Morley College London is an Institute of Adult Learning (IAL) located in central London. It enjoys a distinguished history in British adult education dating back to the early 1880s. The College is both a company limited by guarantee and a registered charity whose Governing Body acts as the board of directors and its members are the trustees of the charity.

The College attracts almost 13,000 individuals to its courses each year and employs more than 550 staff, the majority in part-time teaching roles. It receives public funds through the Education and Skills Funding Agency and undertakes projects and contracts that are funded by a variety of external organisations. In line with its charitable objects it engages in related educational and cultural activities such as public exhibitions, concerts, lectures and other events. The majority of its students pay a fee towards the cost of their course; a sizeable number are pursuing courses for which there are externally accredited examinations or other forms of assessment.

In order to pursue this range of activity the College is required for both regulatory and operational purposes to collect, process and store personal data relating to students, staff and others. The College is, consequently, registered with the Information Commissioner's Register of Data Controllers (ref Z8240054).

3. POLICY STATEMENT

3.1 The College will ensure that information is collected and used fairly, stored safely and not disclosed to any other person unlawfully. Whenever collecting information about people the College will therefore comply with the Data Protection Principles, which are set out in the General Data Protection Regulation (GDPR) and require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, or for scientific or historical research or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals and subject to the College seeking to anonymise data wherever possible; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2 In ensuring that personal data are processed lawfully, the College will only process data under one of the six lawful bases for processing set out in Schedule 6 of the GDPR:

a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3.3 The College recognises that individuals have the following rights:

a) the right to be informed of the information the College holds on them in a concise, transparent, intelligible and easily accessible way. The College will typically make this information available through a Privacy Notice;

b) the right of access to their personal data and supplementary information, and to be aware of and verify the lawfulness of the processing;

c) the right to rectification of their personal data if it is inaccurate or incomplete;

d) the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing (the 'right to be forgotten');

e) the right to 'block' or suppress processing of personal data;

f) the right to data portability: to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to

usability;

g) the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics; and
h) the right not to be subject to a decision when it is based solely on automated processing and produces a legal effect or a similarly significant effect on the individual..

In interpreting the Data Protection Principles and in making judgments on specific matters, the College will take account of the most recent guidance issued by the Information Commissioner's Office (ICO).

4. POLICY OBJECTIVES

To ensure that the College adopts best practice and compliance with legal requirements in its collection, processing and storage of personal data.

5. SCOPE OF POLICY

The policy applies to all governors, employees, students and other users of the College's services. 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 breach of the General Data Protection Regulation or this policy will be considered to be an offence and in that event, the College disciplinary procedures will apply.

As a matter of good practice, other agencies and individuals working with the College, and who have access to personal information, will be expected to have read and to comply with this policy. Employees who deal with external agencies will take responsibility for ensuring that such agencies sign a declaration agreeing to abide by this policy and detailing for how long it has been agreed that any data should be retained. Details of the declaration must be entered on a register to be held by the College's Data Protection Officer.

Any governor, employee or student (or former governor, employee or student) or other individual who considers that the policy has not been followed in respect of the personal data held about them, should initially raise the matter with the Data Protection Officer. If the matter is not resolved it should be raised as a formal grievance or complaint.

6. RESPONSIBILITY STRUCTURE

The College as a body corporate is the Data Controller under the Data Protection Act 1998, and the Governing Body is therefore ultimately responsible for implementation. The Governing Body will appoint a designated Data Protection Officer (who is currently the Clerk to the Governing Body and Company Secretary) to deal with day-to-day matters.

7. PRACTICAL IMPLEMENTATION

7.1 Responsibilities of Governors and Employees

All governors and employees are responsible for:

a) checking that any information that they provide to the College in connection with their office or employment is accurate and up to date;
b) informing the College of any changes to the information which they have provided e.g. changes of address, next of kin, bank details etc.;
c) checking the information that the College will send out from time to time, giving

details of information kept and processed about them;

d) informing the College of any errors or changes; and

e) ensuring that they abide by the College's Information Systems Acceptable Use Policies.

The College cannot be held responsible for any errors unless the individual has informed the College of them.

If and when, as part of their responsibilities, employees collect information about other people they must comply with the guidelines for employees, which are shown at Annex 1. In particular they are responsible for ensuring that:

- any personal data that they hold are kept securely;
- when personal data need to be transmitted, internally or externally, they are transmitted securely; and
- personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Employees should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information must:

- be kept in a locked filing cabinet; or
- be kept in a locked drawer; or
- if it is computerised, be password protected; or
- be kept only on electronic media which are themselves kept securely.

7.2 Responsibilities of Managers

Managers must ensure that:

- all personal data processed within or by members of their curriculum or professional service team are processed according to the Data Protection Principles outlined in 3.1 above;
- privacy notices have been adequately communicated to those whose data are collected, stored or processed;
- consent has been duly obtained where it forms the lawful basis for processing the data;
- individuals have been made aware of their rights under the GDPR;
- any third parties who are commissioned to process personal data on the College's behalf are engaged under a written contract which includes those terms required under the GDPR as set out in guidance issued by the Information Commissioner's Office;
- privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. In planning projects managers must ensure the principles of "privacy by design" are observed and where required a Data Protection Impact Assessment is undertaken in conjunction with the Data Protection Officer; and
- that any breaches of personal data are immediately notified to the Data Protection Officer who will investigate accordingly and where necessary notify the Information Commissioner's Office

7.3 Responsibilities of Students

Students must ensure that all personal data provided to the College are accurate and up to date. They must ensure that changes of address, etc. are notified to the Student Services Team.

Students who use the College's computer facilities may, from time to time, process their own personal data. If they do so they must ensure that they comply with the College's IT Systems Acceptable Use Policy.

7.4 Data Subject Rights

Data Subjects (those individuals about whom the College has information on its records) have rights regarding data processing, and the data that are recorded about them, as set out in 3.3 above.

Governors, employees, students and other persons from or about whom the College has collected personal data therefore have the right to access any personal data that are being kept about them or to receive notification of the information currently being held about them either on computer or in relevant files. Any person who wishes to exercise this right should submit their request to the Data Protection Officer

The College aims to comply with requests for access to personal information as quickly as possible, and will ensure that it is provided within one month unless requests are complex or numerous. If this is the case, the College will inform the individual within one month of the receipt of the request that it needs to extend the period of compliance by a further two months and will explain why the extension is necessary.

The College reserves the right to charge a reasonable fee, taking into account the administrative costs of providing the information, where requests are manifestly unfounded or excessive, in particular because they are repetitive. In exceptional circumstances the College may exercise its right to refuse to respond but will explain its reasons at the latest within one month to the individual, informing them of their right to complain to the supervisory authority and to seek judicial remedy.

7.5 Disclosure

The College will ensure that personal data are not disclosed to unauthorised third parties (including family members, friends, government bodies or the Police) except in the circumstances set out in Part 4 of, and Schedule 7 to, the Data Protection Act 1998 and listed below in which personal data may legitimately be disclosed.

Personal data may be legitimately disclosed where one of the following conditions applies:

a) the individual has given their consent (e.g. a student/employee has consented to the College corresponding with a named third party);
b) the disclosure is in the legitimate interests of the College (e.g. personal information can be disclosed to other College employees if it is clear that those employees require the information to enable them to perform their jobs);
c) the College is legally obliged to disclose the data; or
d) disclosure of data is required for the performance of a contract (e.g. informing a student's employer or sponsor of course changes/withdrawal etc).

The Act permits certain disclosures *without consent* so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;

- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual (this refers to life and death situations).

7.6 Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender or family details. This may be to ensure that the College is a safe place for everyone, or to operate other College policies, such as the Sick Pay Policy or Equality and Diversity Policy. The College may 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 such information in the protection of the health and safety of the individual.

Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and students will be asked to give express consent for the College to do this. All prospective governors, employees and students will therefore be asked to provide consent for the College to process data, regarding particular types of information when an offer of office or employment or a course place is made. A refusal to sign such a form will result in the offer being withdrawn.

7.7 Examination/Assessment Marks

Students who have no outstanding payment of course or assessment fees will be entitled to information about their marks or grades for both coursework and examinations. This may take longer than other information to provide, but will normally be available within 28 days dependent on when the relevant awarding organisation furnishes the College with the information. Where students have outstanding course or assessment fee payments due, the College may withhold certificates, accreditation or references until the full course fees have been paid, or all books and equipment returned to the College.

7.8 Publication of College Information

It is the College's policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- names, photographs and brief biographical details of members of the Governing Body; and
- names and College contact details of Senior Post-holders, Curriculum Managers and Heads of Professional Service departments.

The College also publishes a number of documents that include personal data, and will continue to do so. These personal data include, but are not limited to:

a) names and roles of all members of the Governing Body and its committees.
b) names and job titles of employees.
c) internal telephone/email directory.
d) student exam results including grades.
e) information in course guides (including photographs), reports, newsletters, etc.; and
f) employee/student information on the College website and Intranet (including

photographs)

It is recognised that there might be occasions when an employee, a student, or a Governor requests that their personal details in some of these categories remain confidential or are restricted to internal access. In such instances, the College will comply with the request, subject to any obligations it may have under the Freedom of Information Act, and ensure that appropriate action is taken.

7.8 Retention and Disposal of Data

The College will normally keep personal information only for as long as it is required to retain it for legal or other statutory reasons or as required by the funding or examination body or to meet its responsibilities as an employer (e.g. information regarding pensions, taxation, potential or current disputes or litigation regarding the employment) or education provider. A schedule of retention for different categories of personal information will be maintained by the Data Protection Officer.

Personal data will be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

7.9 Data Security

In order to ensure the protection of personal data held electronically, staff and students are required to adhere to the College's IT Systems Acceptable Use Policies. Breaches of those policies where they concern misuse of personal data will be treated as disciplinary matters.

The College's IT Services Manager is responsible for ensuring that there are appropriate and adequate security measures in place including, as part of the College's Business Continuity arrangements, an IT Recovery Plan.

Should there be a breach of security the College will notify any individuals whose personal data may have been disclosed to a third party as a result of the breach and will consider whether the breach warrants reporting to the Information Commissioner's office under the ICO's Guidance on Notification of Data Security Breaches.

7.10 Use of CCTV

To protect College premises and the property of employees and students, closed-circuit television cameras are in operation in various parts of the College. Images of people and information about people derived from images are covered by the Data Protection Act.

Personal data obtained through the use of CCTV will only be processed in accordance with the ICO's CCTV Code of Practice and in particular:

a) any monitoring will be carried out only by a limited number of specified employees;
b) the recordings will be accessed only by the Principal, The Vice Principal, the Premises Manager and other duly authorised personnel, including those responsible for IT Services, Reception and Security;
c) personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete; and
d) employees involved in monitoring will maintain confidentiality in respect of personal data.

8. COMMUNICATION AND TRAINING

The policy will be communicated to staff and students through the College's internal committee structures and via the College's intranet and website.

9. REVIEW AND MONITORING OF POLICY

The Information and Data Protection Policy will be reviewed on a quadrennial basis by the Governing Body. The Senior Management Team is responsible for monitoring the implementation of the Policy via reports from the Data Protection Officer and relevant members of the College Management Team.

Annex 1

Employee Guidelines for Data Protection

1. Many employees 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 role. Other employees may need to process data about fellow members of staff or other individuals. The College will ensure through registration and recruitment procedures, that all students give their consent to such processing, and are notified of the categories of processing, as required by the 1998 Act. The information that employees 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 attendance, or about course work marks, grades and associated comments or performance at work; and
   - notes of personal supervision, including matters about behaviour and discipline.
2. Information about an individual's physical or mental health; sexual orientation; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. If employees need to record this information where agreed college policies and practices require or encourage the sharing of this information, they should use College standard forms and templates.
3. All employees have a duty to make sure that they comply with the Data Protection Principles, which are set out in the College Information and Data Protection Policy. In particular, employees must ensure that records are:

   (a) accurate;

   (b) up-to-date;

   (c) fair; and

   (d) kept and disposed of safely, and in accordance with College policy.
4. Employees must not disclose personal data relating to any individual to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the Data Protection Officer, or in line with College policy.
5. Employees must not disclose personal data relating to any individual to any other employee except with the authorisation or agreement of the Data Protection Officer, or in line with College policy.
6. Before processing any personal data, all employees should consider the following checklist:
   - 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 are 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 employee to collect and retain the data?
   - Have you reported the fact of data collection to the authorised person within the required time?