MORLEY COLLEGE LONDON

Data Protection Policy

POLICY OWNER: Data Protection Officer
APPROVAL: Governing Body
APPROVED: 1 April 2019
NEXT REVIEW: March 2023 or at such earlier date as may be required by changes in legislation

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
Sex
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*
Association of Colleges: *Model Documents for Colleges*

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)

The draft Policy should be reviewed by lawyers before being submitted to the Board for approval

DATA PROTECTION POLICY

1. INTRODUCTION AND PURPOSE

Morley College London needs to collect and maintain certain Personal Data relating to its governors, employees, students and other users of its services, visitors and contractors to allow it to conduct its business and to monitor, for example, performance, achievements, and health and safety. It is also necessary for the College to process Personal Data so that governors, employees and students can be recruited, employees paid, contractors engaged, 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, contractors, 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, contractors and students, Friends of Morley, past and potential future donors, Individuals involved in fund-raising and other Individual stakeholders.

The College's reputation and the delivery of its mission are dependent on the ways in which it manages and protects Personal Data. Ensuring the confidentiality and integrity of those data is an important responsibility of all members of the College community. The College also recognises that controls around the collection, use, retention and destruction of Personal Data are essential to ensure that the College complies with its obligations under Data Protection Laws, in particular the General Data Protection Regulation and the Data Protection Act 2018.

The College has adopted and implemented this Data Protection Policy to ensure that all College Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects the data from individuals directly, or where the data are provided to the College by third parties. It also sets out rules on how the College handles uses, transfers and stores Personal Data. It applies to all Personal Data stored electronically, in paper form, or otherwise.

2. DEFINITIONS

In this Policy the following expressions have the meanings given:

College Personnel: any College governor, employee, worker or contractor who may access any of the Personal Data held by the College (including consultants and temporary personnel hired to work on the College's behalf).

Data Controller: any entity (such as a company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Data Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data of which the College is the Controller include employee details and information that the College collects relating to students. It is a common misconception that individuals within organisations are the Controllers. That is not the case: it is the organisation itself that is the Controller.

Data Protection Laws: the General Data Protection Regulation (Regulation (EU) 2016/679) (**'GDPR'**), all applicable laws relating to privacy and to the collection and use of Personal Data, including, in the UK, the Data Protection Act 2018 ('the Act'), and any applicable codes of practice issued by a regulator.

Data Protection Officer (DPO): the person designated by the Governing Body to monitor implementation and to provide independent advice to the Governing Body and the Senior Management Team on data protection matters. The current DPO is the Clerk to the Governing Body and Company Secretary. The name, telephone number and email address of the DPO are included in every Privacy Notice.

Data Subject: an Individual whose Personal Data may be requested, held or processed by the College.

EEA: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

ICO: the Information Commissioner's Office, the UK's data protection regulator.

Individuals: Living persons who can be identified, directly or indirectly, from Personal Data. For example, an Individual could be identified directly by name, or indirectly by a combination of gender, job role and office location if these data were sufficient to enable the Individual's identity to be deduced. Individuals include governors, employees, students, and potential students. Individuals may also include partnerships and businesses that operate as sole traders.

Personal Data: Any information about an Individual that identifies them or allows them to be identified if used in conjunction with other information that is held. Personal Data are defined broadly and include names, addresses, email addresses (including in a business context, business email addresses such as firstname.surname@organisation.com), IP addresses and other more sensitive types of data such as trade union membership, genetic data, religious belief or criminal record. These more sensitive types of data are given extra protection by Data Protection Laws.

Privacy Notice: A notice provided to Individuals whose Personal Data the College is collecting or receiving, informing them of the purposes for which the College will process their Personal Data, the retention periods for those data and with whom the data will be shared. The College has separate privacy notices in place for governors, for staff and applicants and for students and prospective students, Friends of Morley, visitors and other users of the College's services.

Processor: Any entity (whether a company, organisation or person) that accesses or uses Personal Data on the instruction of a Controller. A Processor may be a third party organisation that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

Special Categories of Personal Data: Personal Data that reveal an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, inherited or acquired genetic characteristics (genetic data),physical or mental health, physical, physiological or behavioural characteristics such as facial images or fingerprints (biometric data), sex life or sexual orientation. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

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 around 12,000 students to its courses each year and employs more than 600 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 fees towards the costs of their courses; 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, governors, 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 data are collected and used fairly, stored safely and not disclosed to any other person unlawfully. Whenever collecting information about Individuals the College will therefore comply with the Data Protection Principles, which are set out in the 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 that 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 they will be processed solely for archiving purposes in the public interest, scientific or historical research purposes 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 the College to process their Personal Data for one or more specific purposes.

b) Contract: the processing is necessary for a contract the College has with the

Individual, or because the Individual has asked the College to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for the College 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 the College to perform a task in the public interest or for the College's official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for the College's 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 to any data that the College processes as a public authority to perform its official tasks.)

3.3 Special Categories of Personal Data are subject to additional controls above and beyond those that apply to all Personal Data. The College will only process data in these special categories under the conditions set out in Article 9(2) of the GDPR, as modified by Schedule 1 of the Act, which can be summarised as follows:

a) the Individual has given explicit consent.

b) processing is necessary to comply with employment and social security obligations

c) processing is necessary to protect the vital interests of the Individual or another person and the Individual is not physically or legally able to give consent

d) [applies only to bodies with philosophical, political, religious or trade union aims]

e) the Individual has manifestly made the data public

f) processing is necessary for the establishment or defence of legal claims

g) processing is necessary for reasons of substantial public interest

h) processing is necessary for reasons connected with the health of the Individual

i) processing is necessary for public health reasons

j) processing is necessary for archiving, research or statistical purposes

In processing Special Categories of Personal Data, College Personnel should refer to the detailed guidance to be published by the ICO; in the absence of that detailed guidance, advice should be sought from the Data Protection Officer.

Personal Data that relate to criminal convictions or offences or to related security measures are also subject to additional controls, which are broadly in line with those that apply to special categories of Personal Data. In processing data of this type, College Personnel should again refer to the detailed guidance to be published by the ICO; in the absence of that detailed guidance, advice should be sought from the Data Protection Officer.

3.4 The College recognises that Individuals have the following rights:

a) the right to be informed of the data that 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 they are inaccurate or incomplete;

d) the right to request the deletion or removal of Personal Data where there is no compelling reason for their 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, where it is processed by automated means;
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 ICO.

4. POLICY OBJECTIVES

To ensure that the College adopts and can demonstrate that it has adopted best practice and compliance with legal requirements in its collection, processing and storage of Personal Data.

5. SCOPE OF POLICY

This Policy applies to all College Personnel, students and other users of the College’s services. It 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 Data Protection Laws 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 Data, will be expected to have read and to comply with this Policy. College Personnel 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 Data Subject 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 and the Governing Body is therefore ultimately responsible for implementation. The Governing Body has delegated day-to-day responsibility for implementation of the Policy to the Principal. It has appointed a Data Protection Officer to monitor implementation and to provide independent advice to the Governing Body and the Senior Management Team on data protection matters.

The Data Protection Officer shall directly report to the Governing Body and shall:

a) inform and advise the College and its employees who carry out processing of their obligations under Data Protection Laws;
b) monitor compliance with Data Protection Laws and this Policy and any other data protection policies of the College, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and related audits;

c) report annually to the Governing Body on the implementation of this Policy;
d) cooperate with the ICO; and
e) act as the contact point for the ICO on issues relating to processing.

7. PRACTICAL IMPLEMENTATION

7.1 Responsibilities of College Personnel

All College Personnel are responsible for:

a) checking that any data that they provide to the College in connection with their office, employment or service contract are accurate and up to date;
b) informing the College of any changes to the data that they have provided, such as changes of address, next of kin or bank details;
c) checking the information that the College will send out from time to time, giving details of data held and processed that relate directly to 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, College Personnel collect Personal Data they must comply with the Data Protection Guidelines for College Personnel, 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 in accordance with the College's IT Systems Acceptable Use Policy; and
- Personal Data are 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 Data must:

- if held in digital form:
    - be password protected; and
    - be kept only on electronic media which are themselves kept securely; and
- if held on paper:
    - be kept in a locked filing cabinet; or
    - be kept in a locked drawer.

7.2 Responsibilities of Managers

Managers must ensure that:

- all Personal Data processed within or by members of their curriculum or professional service teams 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 Data Protection Laws;
- If at any time a change is contemplated in how any Personal Data are used, they inform the DPO who will decide whether the intended use requires any amendments to be made or any other controls applied;
- 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 Data Protection Laws as set out in guidance issued by the ICO;
- privacy and data protection are key considerations both in the early stages of any project and throughout its life cycle. In planning projects, managers must ensure that the principles of "privacy by design" are observed and that, where required, a Data Protection Impact Assessment is undertaken in conjunction with the Data Protection Officer;
- any breaches of Personal Data are immediately notified to the Data Protection Officer who will investigate accordingly and where necessary notify the ICO. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is not just about losing personal data and can include:
  - access by an unauthorised third party;
  - deliberate or accidental action (or inaction) by a controller or processor;
  - sending personal data to an incorrect recipient;
  - computing devices containing personal data being lost or stolen;
  - alteration of personal data without permission; and
  - loss of availability of personal data; and
- all Personal Data processed within or by members of their curriculum or professional service teams are reviewed at least annually and a retention schedule prepared in accordance with the College's Information and Data Retention Policy.

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 in their Personal Data, including changes of address, 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 have rights in relation to the data that are held about them, and how those data are processed, as set out in 3.4 above. The College will use all Personal Data in accordance with the rights given to Individuals under Data Protection Laws, and will ensure that it allows Individuals to exercise those rights, including but not limited to the following:

<u>Subject access requests</u>

Governors, employees, students and other persons from or about whom the College has collected Personal Data have the right to receive confirmation of and to access

any Personal Data that are held about them in digital, paper or any other form. Any person who wishes to exercise this right should submit a request to the Data Protection Officer.

The College aims to comply with requests for access to Personal Data 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 up to 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 data requested, where a request is manifestly unfounded or excessive, or where there are repeated requests for the same data. In exceptional circumstances the College may exercise its right to refuse to respond but will explain its reason to the person making the request within one month of the receipt of the request, informing them of their right to complain to the supervisory authority and to seek judicial remedy.

Right of Erasure (right to be forgotten)

Data Subjects may request the erasure of Personal Data concerning them where:

- the use of the Personal Data is no longer necessary;
- the Data Subject's consent is withdrawn and there is no other legal ground for the processing;
- the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the Personal Data have been unlawfully processed; or
- the Personal Data have to be erased to enable compliance with a legal obligation.

In a marketing context, where Personal Data are collected and processed for direct marketing purposes, the Data Subject has a right to object to processing at any time. Where the Data Subject objects, the Personal Data must not be processed for such purposes.

Right of Data Portability

Data Subjects have the right to request that data concerning them are provided to them in a structured, commonly used and machine readable format where:

- the processing is based on consent or on a contract; or
- the processing is carried out by automated means.

Right of Rectification and Restriction

Data Subjects have the right to request that any Personal Data are rectified if inaccurate and that in certain circumstances use of their Personal Data be restricted to particular purposes.

7.5 Sensitive Data

Sometimes it is necessary to process data 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 data relating to particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only process such data where one of the relevant conditions referred to in Section 3.3 above has been met.

7.6 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) other information published on the College website or Intranet (including photographs).

It is recognised that there may be occasions when a member of College Personnel, a student or another Data Subject requests that their Personal Data 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.

7.7 Retention and Disposal of Data

The College will normally keep Personal Data only for as long as it is required to retain them for legal or other statutory reasons or as required by the funding or examination body or to meet its responsibilities as an employer (for example, in relation to data regarding pensions, taxation, potential or current disputes or litigation regarding the employment), contractor or education provider. A schedule of retention for different categories of Personal Data 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 (for example, by shredding, disposal as confidential waste or secure electronic deletion).

7.8 Data Security

In order to ensure the protection of Personal Data held electronically, College Personnel 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.

7.9 Use of CCTV

To protect College premises and the property of College Personnel, students and other users of the College's premises, 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 Laws.

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 College Personnel;

b) the recordings will be accessed only by the Principal, the Vice Principal, the Premises Manager and other duly authorised College 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) College Personnel involved in monitoring will maintain confidentiality in respect of Personal Data.

7.10 Appointing contractors who access the College's Personal Data

If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only makes the appointment where the College has carried out sufficient due diligence and has appropriate contracts in place.

Data Protection Laws require that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of Individuals. This means that data protection due diligence (and especially security due diligence) should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

The College is considered as having appointed a Processor where it engages a contractor to perform a service and as part of that service the contractor may get access to some of the College's Personal Data. The College, as Controller, remains responsible for what happens to the Personal Data.

Any contract appointing a Processor must be in writing and must contain the following obligations as a minimum:

- to act only on the written instructions of the Controller;
- not to export Personal Data without the Controller's instruction;
- to ensure that staff are subject to confidentiality obligations;
- to take appropriate security measures;
- only to engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of data breaches and Data Protection Impact Assessments;
- in so far as possible, to assist the Controller to fulfil its obligations to respond to requests from Individuals exercising their rights, including subject access requests;
- to delete/return all Personal Data as requested at the end of the contract;

- to submit to audits and provide information about the processing; and
- to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

In addition the contract should set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the types of Personal Data and categories of Individuals; and
- the obligations and rights of the Controller.

7.11 Marketing and Consent

The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner. Marketing consists of any advertising or marketing communication that is directed to particular Individuals.

College Personnel also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside the Data Protection Laws. The PECR apply to direct marketing (communications directed to particular Individuals) and cover any advertising/marketing material. The PECR apply to all forms of electronic communication, including telephone calls, emails, texts and faxes, and apply even when the College is not processing any Personal Data. The College will issue guidance on marketing and the PECR.

7.12 Automated Decision Making and Profiling

Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals:

- **Automated Decision Making** happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
- **Profiling** happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

The College can only carry out any Automated Decision Making or Profiling if it is confident that it is complying with Data Protection Laws. If College Personnel wish to carry out any Automated Decision Making or Profiling they must obtain the prior approval of the Data Protection Officer.

The College does not carry out Automated Decision Making or Profiling in relation to its employees.

7.13 Data Protection Impact Assessments

The GDPR introduces a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment (DPIA). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data that need to be considered before a new product/service/process is rolled out. The process is designed to:

- describe the collection and use of Personal Data;
- assess its necessity and its proportionality in relation to the purposes;
- assess the risks to the rights and freedoms of individuals; and

- evaluate the measures that are proposed to address the risks.

A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to carry out a DPIA at an early stage in the process so that the College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

Situations where the College may have to carry out a DPIA include the following (please note that this list is not exhaustive):

- large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
- large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
- systematic monitoring of public areas on a large scale, for example by CCTV cameras.

All DPIAs must be reviewed and approved by the Data Protection Officer.

7.14 Data Transfer

Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the College appoints a supplier outside the EEA or with group companies outside the EEA that may give access to the Personal Data to staff outside the EEA.

So that the College can ensure it is compliant with Data Protection Laws College Personnel must not export Personal Data outside the EEA without the approval of the Data Protection Officer.

8. COMMUNICATION AND TRAINING

All governors, employees and contractors will be made aware of this Policy on joining the College. The Policy will be communicated to College Personnel and students through the College's internal committee structures and via the College's intranet and website.

9. REVIEW AND MONITORING OF POLICY

The 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

Data Protection Guidelines for College Personnel

1. Many College Personnel 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 College Personnel may need to process data about fellow members of College Personnel or other Individuals. The College will ensure through registration and recruitment procedures that all students and College Personnel give their consent to such processing, and are notified of the categories of processing, as required by the Data Protection Laws. The information that College Personnel deal with on a day-to-day basis will be 'standard' and will cover categories such as:
   - general personal details such as names and addresses;
   - 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. Personal Data that reveal an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, inherited or acquired genetic characteristics (genetic data),physical or mental health, physical, physiological or behavioural characteristics such as facial images or fingerprints (biometric data), sex life, sexual orientation or criminal convictions or offences or related security measures are sensitive. They can only be collected and processed either with the Data Subject's explicit consent or in a very limited range of other circumstances. If College Personnel need to record such data where agreed College policies and practices require or encourage its recording, they should use College standard forms and templates.
3. All College Personnel 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, they 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.

   College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.
4. College Personnel must not release or disclose any Personal Data (whether in speech, by telephone, by email or by any other means):

   (a) outside the College; or

   (b) inside the college to College Personnel not authorised to access the data

   without specific authorisation from their manager or the Data Protection Officer.
5. College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College
6. Before processing any Personal Data, all College Personnel should consider the following checklist:
   - Do you really need to record the data?
   - Do the data fall within one of the Special Categories of Personal Data or relate to a criminal conviction or offence or to any related security measures?

- If so, are you satisfied that at least one of the conditions for processing such data is met (including, where no other condition is met, the Data Subject's express consent)?
- Has the Data Subject been told that data of this type will be processed?
- Are you authorised to collect/store/process the data?
- If so, 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 (or, for certain types of data, express consent) to process, are you satisfied that you have another lawful basis for processing the data?
- Have you reported the fact of data collection to the authorised person within the required time?