# Moulton College Data Protection Policy

| | | | |
|---|---|---|---|
| **Policy Reference** | DP-01 | | |
| **Issue Date** | 20 October 2021 | **Review Date** | 20 October 2023 |

# Document Control

### About This Document

This document details The Colleges approach to protecting the confidentiality and integrity of personal data controlled and processed in any and all aspects of its operations.

**Document Control**

| | |
|---|---|
| **Owner** | Chief Finance Officer |
| **Audience** | All Moulton College Staff including contractors, consultants, and temporary personnel |
| **Confidentiality** | Low |

**Version Control**

| Version | Description/Changes | By | Date |
|---|---|---|---|
| 1.0 | Initial Version | GB | 17.05.18 |
| 1.1 | Revised following DPO Review | GB | 12.06.19 |
| 1.2 | Annual approval | GB | 06.10.20 |
| 1.3 | Annual approval | AJB | 8/10/21 |

**Approval**

| Approved By | Meeting Date | Next Review |
|---|---|---|
| Senior Leadership Team | 20/10/2021 | 20/10/2023 |
| Corporation Board | | ?/10/2023 |

**Related Policies**

| Policy | Relationship | |
|---|---|---|
| Rights of Individuals Policy | Direct | |
| Data Breach Notification Policy | Direct | |
| Retention Policy | Direct | |
| Destruction of Confidential Paper Records | Indirect | |
| CCTV | Indirect | |
| Prevent | Indirect | |
| Safeguarding | Indirect | |
| Acceptable Use of IT | Indirect | |
| | | |

TABLE OF CONTENTS

## 1. OVERVIEW

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

As an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, alumni, governors, parents, clients and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Legislation and in particular its obligations under Article 5 of UK GDPR.

The College has implemented this Data Protection Policy to ensure 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.

College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of the College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of College Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Lead, who is responsible for ensuring the College's compliance with this Policy. They can be contacted as follows:

**Email:** dataprotection@moulton.ac.uk
**Phone:** 0 - Reception

## 2. ABOUT THIS POLICY

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 it from individuals itself, or where it is 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.

This policy supplements our other policies such as those relating to Internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being implemented.

## 3. GOVERNANCE

The corporation board will monitor this policy and review it annually. However, they have devolved approval of the directly related policies to the Senior Leadership Team to ensure that the policies and processes can be dynamically updated as required.

## 4. DEFINITIONS

4.1. **College** – Moulton College and its wholly owned subsidiaries

4.2. **College Personnel** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

4.3. **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Legislation. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.

A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

**Data Protection Legislation** –Data Protection Legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time. We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

**Data Protection Officer –** Our Data Protection Officer is the DPO Centre Ltd. Our data protection team can be contacted at: dataprotection@moulton.ac.uk or ext 2555

4.4. **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.

4.5. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

4.6. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders. They may also be referred to as 'data subjects' or 'natural persons'.

4.7. **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as health/medical data, trade union membership, genetic data and religious beliefs. These more sensitive types of data are called

"Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Legislation.

4.8. **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

A Processor is a third party 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.

4.9. **Special Categories of Personal Data** – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

## 5. ACCOUNTABILITY

The College must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The College is responsible for, and must be able to demonstrate compliance with, the data protection principles.
We must therefore apply adequate resources and controls to ensure and to document UK GDPR compliance including:

5.1. Appointing a suitably qualified Data Protection Officer

5.2. Implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;

5.3. Integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;

5.4. Training staff on compliance with Data Protection Law and keeping a record accordingly; and

5.5. Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

## 6. COLLEGE PERSONNEL'S OBLIGATIONS

6.1. All College Personnel who process personal data about students, staff, applicants or any other individual must comply with this policy.

6.2. 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.

6.3. College Personnel must not release or disclose any Personal Data:

6.3.1. outside the College; or

6.3.2. inside the college to College Personnel not authorised to access the Personal Data,

without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

6.4. College Personnel must ensure that personal data is kept in accordance with the College's retention schedule

6.5. 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

6.6. College Personnel must ensure that any data protection breaches are swiftly brought to the attention of their Line Manager or the Data Protection Coordinator and that they support with resolving breaches where necessary

6.7. College Personnel must ensure that any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Coordinator.

6.8. College Personnel must undergo mandatory data protection training. There are online resources for this – pls contact the Data Protection Coordinator for detailed information about the training available.

6.9. All systems and processes will be reviewed regularly to ensure staff comply with this.

## 7. DATA PROTECTION PRINCIPLES

7.1. When using Personal Data, Data Protection Legislation require that the College complies with the following principles. These principles require Personal Data shall be:

7.1.1. processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

7.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

7.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed ('data minimisation');

7.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible ('accuracy');

7.1.5. kept for no longer than is necessary for the purposes for which it is being processed ('storage limitation');

7.1.6. 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 ('integrity and confidentiality');

7.1.7. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

7.2. These principles are considered in more detail in the remainder of this Policy.

7.3. The 7th Accountability principle requires the College to demonstrate it complies with all the above principles. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

## 8. LAWFUL USE OF PERSONAL DATA

8.1. In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing]

8.2. In addition when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data].

8.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 8.1 and 8.2. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change. If College Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

8.4. When processing any personal data (information which does or may identify a living individual), we must establish a lawful basis for processing data. Employees must ensure that any data they are responsible for managing or working with has a written lawful basis approved by the DPO.

At least one of the following conditions must apply whenever we process personal data:

I. **Consent**
We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

II. **Contract**
Processing is necessary to fulfil or prepare a contract for the individual.

III. **Legal obligation**
Processing is necessary to meet a legal obligation (excluding a contract).

IV. **Vital interests**
Processing is necessary to protect a person's life or in an urgent medical situation.

V. **Public function**
Processing is necessary to carry out a public function, a task of public interest, or the function has a clear basis in law assigned to us.

VI. **Legitimate interest**
Processing is necessary for the business/organisation's legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

## Deciding which condition to rely on

- If you are making an assessment of the lawful basis of processing, you must first establish that the processing is necessary to achieve your purpose. This means the processing must be a targeted, appropriate way of achieving a stated purpose.
- You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means that doesn't require the use of the personal data.
- You must also only use the minimum data required to achieve the purpose (e.g. don't use a full date of birth if an age or age range will do).
- Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.
- Consider the following factors and document your answers:
- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?
- Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions. All data processing must be recorded reported to and recorded by the Data Protection Officer
- We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a Privacy Notice. This applies whether we have collected the data directly from the individual, or from another source. You must record how individuals are to be informed and for written communications keep a copy of the wording used. This must be reported to the DPO who will approve wording and include relevant information in Enterprise's overall Privacy Notice published on our website.
- If no other lawful basis applies, you may be able to rely on Legitimate Interests. If this is the case a Legitimate Interests Assessment (LIA) must be undertaken and documented. If you need to conduct an LIA, you must conduct the DPO who will assist in conducting and approving the assessment. Note that in most

cases, Legitimate Interests is only likely to be a suitable legal basis where the processing has little likelihood of affecting the rights or freedoms of a data subject.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

8.5.

## 9. TRANSPARENT PROCESSING – PRIVACY NOTICES

9.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice.

9.2. If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

9.3. If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College Personnel therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the College Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

## 10. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

10.1. Data Protection Legislation require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 9 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

10.2. All College Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

10.3. All College Personnel that obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require College Personnel to independently check the Personal Data obtained.

10.4. In order to maintain the quality of Personal Data, all College Personnel that access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this

does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

10.5. The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Legislation. The College has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

## 11. PERSONAL DATA RETENTION – MUST NOT BE KEPT FOR LONGER THAN NEEDED

11.1. Data Protection Legislation require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

11.2. The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

11.3. If College Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College Personnel have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

## 12. DATA SECURITY

The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

## 13. DATA BREACH

13.1. Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens, it constitutes a Personal Data breach and College Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 13.2 and 13.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event of Personal Data breaches.

13.2. Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third

party, they are more likely to occur as a result of something someone internal does, e.g sending an email to the wrong person, leaving documents on the photocopier etc..

13.3. There are three main types of Personal Data breach which are as follows:

13.3.1. **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

13.3.2. **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

13.3.3. **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

## 14. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA

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

14.2. One requirement of UK GDPR is that a Controller must only use Processors who meet the requirements of the UK GDPR and protect the rights of individuals. This means that data protection 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.

14.3. Any contract appointing a Processor must be in writing. The data protection clauses may be in the main commercial contract or in a separate Data Processing Agreement.

14.4. UK GDPR requires the contract with a Processor to contain the following obligations as a minimum:

14.4.1. to only act on the written instructions of the Controller;

14.4.2. to not export Personal Data without the Controller's instruction;

14.4.3. to ensure staff are subject to confidentiality obligations;

14.4.4. to take appropriate security measures;

14.4.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

14.4.6. to keep the Personal Data secure and assist the Controller to do so;

14.4.7. to assist with the notification of Data Breaches

14.4.8. to assist with Data Protection Impact Assessments;

14.4.9. to assist with Subject Access Requests/individuals rights;

14.4.10. to delete/return all Personal Data as requested at the end of the contract;

14.4.11. to submit to audits and provide information about the processing; and

14.4.12. to tell the Controller if any instruction is in breach of the UK GDPR or other data protection law.

14.5. In addition the contract should set out:

14.5.1. The subject-matter and duration of the processing;

14.5.2. the nature and purpose of the processing;

14.5.3. the type of Personal Data and categories of individuals; and

14.5.4. the obligations and rights of the Controller.

## 15. INDIVIDUALS' RIGHTS

***Note: Please refer to the accompanying standard Rights of Individuals Policy and Rights of Individuals Procedure.***

15.1. UK GDPR gives individuals more control about how their data is collected and stored and what is done with it. It is extremely important that Staff understand the rights individuals have under this legislation and can recognise when they are being exercised as requests to the College. .

15.2. The different types of rights of individuals are reflected in this paragraph.

15.3. **Right to be Informed**

- We will provide privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- We must keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

15.4. **Right of Access (Subject Access Requests)**

15.4.1. Individuals have the right under the UK GDPR to ask a College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible 2 month extension if it is a demonstrably complex request).

**How we deal with subject access requests**

- We must provide the individual with a copy of the information they requested, free of charge. This must occur without delay, and within one month of receipt of the request. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.
- If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO before extending the deadline.
- We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.
- Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

15.4.2. Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

15.5. **Right of Erasure (Right to be Forgotten)**

15.5.1. This is a limited right for individuals to request the erasure of Personal Data concerning them where:

15.5.1.1. the use of the Personal Data is no longer necessary;

15.5.1.2. their consent is withdrawn and there is no other legal ground for the processing;

15.5.1.3. the individual objects to the processing and there are no overriding legitimate grounds for the processing;

15.5.1.4. the Personal Data has been unlawfully processed; and

15.5.1.5. the Personal Data has to be erased for compliance with a legal obligation.

**How we deal with the right to erasure**

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation, for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- For the exercise or defence of legal claims

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

15.6. **Right of Data Portability**

15.6.1. An individual has the right to request that data concerning them is provided to them or a third party, in a structured, commonly used and machine readable format where:

15.6.1.1. the processing is based on consent or on a contract; and

15.6.1.2. the processing is carried out by automated means

15.6.2. This right isn't the same as subject access and is intended to make it easy for a data subject authorised third party to receive a subset of an individual's data, in a usable format.

**Data portability requests**
We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month from receipt of the request. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO first.

15.7. **The Right to object**

Individuals have the right to object to their data being used on grounds relating to their particular situation.
We must cease processing unless:
We have legitimate grounds for processing which override the interests, rights and freedoms of the individual
The processing relates to the establishment, exercise or defence of legal claims
We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice.
We must offer a way for individuals to object online.

15.8. **The Right to Restrict Automated Profiling or Decision Making**

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract
- We have gained the individual's explicit consent
- We are otherwise authorised by law

In these circumstances, we must:

- Give individuals detailed information about the automated processing
- Offer simple ways for them to request human intervention or challenge any decision about them
- Carry out regular checks and user testing to ensure our systems are working as intended

15.9. **Right of Rectification**

15.9.1. Individuals are also given the right to request that any Personal Data is rectified if inaccurate or incomplete.

15.9.2. This will be done without delay, and no later than one month from the request. This can be extended to two months with permission from the DPO.

15.10. Right to Restrict Processing

We will comply with any request to restrict, block, or otherwise suppress the processing of personal data.

We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

15.11. The College will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Legislation, and will ensure that it allows Individuals to exercise their rights in accordance with the College's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which College Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

## 16. MARKETING AND CONSENT

16.1. The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Legislation require that this is only done in a legally compliant manner.

16.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. The UK GDPR requires us to be transparent about our marketing activity and the lawful basis we rely on, including:

16.2.1. providing comprehensive detail in our privacy notices, including for example whether profiling takes place; and

16.2.2. recording the basis upon which we contact individuals, e.g. legitimate interest or where we can demonstrate an individual's "clear affirmative consent".

16.3. Staff also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection regulations. PECR apply to direct electronic marketing i.e. an email directed to particular individuals that includes any advertising/marketing material. It applies to all electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data.

16.4. Consent is central to electronic marketing. We would recommend that best practice is to provide an opt-in box for the individual to actively tick. Pre-ticked boxes are not acceptable.

16.5. Alternatively, the College may be able to market using a “soft opt in” if the following conditions were met:

16.5.1. contact details have been obtained in the course of a sale (or negotiations for a sale);

16.5.2. the College are marketing its own similar services to that which the individual has previously used or expressed an interest in; and

16.5.3. the College gives the individual a simple opportunity to refuse or to opt out of the marketing, both when first collecting the details and in every message after that.

16.6. Under Data Protection Legislation 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.

16.7. Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Legislation. If College Personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

## 17. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

17.1. The UK GDPR introduced 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 Screening Questionnaire should be completed as early as practical in the project lifecycle for all new processes, products or services (internal or external) where personal data may be processed (e.g. a new inhouse report that will be regularly used, a new cloud-based service used to support learning, a new

Occupational Health service/provider etc.). Completed DPIA Screening Questionnaires should be sent to the Data Protection Lead who will then assess whether a full DPIA is required. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

17.1.1. describe the collection and use of Personal Data;

17.1.2. assess its necessity and its proportionality in relation to the purposes;

17.1.3. assess the risks to the rights and freedoms of individuals; and

17.1.4. identify measures to reduce/remove the risks.

17.2. 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.

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

17.4. Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College should complete a DPIA Screening Questionnaire as part of the project initiation process. The College will then be in a position to carry out a DPIA, if required, at an early stage in the process. This will allow the College to 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.

17.5. Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

17.5.1. 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;

17.5.2. 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

17.5.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.

17.6. All DPIAs must be reviewed and approved by the Data Protection Officer.
All queries or completed DPIA Screening Questionnaires should be sent to: **dataprotection@moulton.ac.uk** or alternatively, call **ext 2555**, if you have any queries relating to this

17.7.

## 18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

18.1. Data Protection Legislation imposes strict controls on Personal Data being transferred outside the UK and EEA. Transfer includes sending Personal Data outside the UK and EEA, but also includes storage of Personal Data or access to

it outside the UK and EEA. This must be considered whenever the College appoints a supplier outside the UK or EEA or the College appoints a supplier with group companies outside the UK or EEA which may give access to the Personal Data to staff outside the UK or EEA.

18.2. So that the College can ensure it is compliant with Data Protection Legislation College, Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

18.3. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

## 19. SHARING DATA

19.1. In the absence of Consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to the College (e.g. students' parents, members of the public, private property owners).

19.2. Some bodies have a statutory power to obtain information (e.g. regulatory bodies such as the Health & Care Professions Council, the Nursing and Midwifery Council, government agencies such as the Child Support Agency). You should seek confirmation of any such power before disclosing personal data in response to a request. If you need guidance, please contact the data protection team on **dataprotection@moulton.ac.uk**

19.3. Disclosure to the Police is permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should ask for a formal request for personal data from the police that states the relevant exemption that applies. If you need guidance, please contact the Data Protection officer.

# Equality Impact Assessment (EIA)

Please complete both sides of this Equality Impact Assessment and ensure that the latest copy of this is recorded as part of the appendices of the specific policy.

| | |
|---|---|
| **Policy Reference and Name** | DP01 General Data Protection Policy |
| **Assessment date** | 8 September 2021 |
| **Completed by** | Director of Student Services |
| **What are the aims of the policy?** | To protect the confidentiality and integrity of personal data |
| **Who does the policy affect?** | Students, internal and external partners. |
| **Who is involved in implementing the policy?** | Director of Student Services, Student Services Coordinator, GDPR Administrator, MIS Manager/team, IT Team |
| **What information is currently available about the impact of this policy and its associated procedures?** | Logs and records are now being kept to measure impact of policy. |
| **Do you need more information to help you make an assessment about the impact of this policy and its associated procedures?** | The above logs will identify those effected by issues this policy seeks to address. |
| **Do you have any examples that show how this policy will have a positive impact on any of the equality characteristics listed in the table below?** | No |
| **Which other policies does this policy link with?** | Data retention policy, Destruction of Confidential paper records, Personal data breach notification policy, Rights of Individuals Policy |
| **What consultation has taken place in the development of this policy?** | Discussions with Director of Student Welfare / DPO |

**Use the table below to assess the impact of this policy on each of the listed characteristics. Your decision must be evidence based.** Sources of evidence might include success rates, achievement gaps, application and enrolment data, student voice, consultation outcomes, recruitment and employment data, customer feedback or complaints, meeting minutes.

| Characteristic<br>(These characteristics are protected under the Equality Act 2010) | Negative impact?<br>Y / N | Evidence to support your impact assessment decision | Requires further action?<br>Y/N |
|---|---|---|---|
| Age | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Disability | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Race | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Gender, inc. re-assignment | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Sexual orientation | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Religion / belief | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Pregnancy / maternity | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Marriage / civil partnership | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |
| Socio-economic | N | Data used by the college is protected appropriately and where used all references to individuals removed. | N |

## Overall EIA judgement

| Select | |
|---|---|
| ✓ | *No change required*<br>The assessment is that the policy is/will be robust. There is no evidence of potentially unlawful discrimination and all reasonable opportunities to advance equality and foster good relations have been taken, subject to continuing monitoring and review |
| | *Adjust the policy or practice*<br>This involves taking steps to remove any barriers, to better advance equality and/or to foster good relations. This may involve removing or changing the aspect of the policy that creates any negative or unwanted impact. It may also involve introducing additional measures to reduce or mitigate any potential negative impact |
| | *Continue the policy*<br>This means adopting/continuing with the policy despite the potential for adverse impact. Set out the rationale for this decision, including how the decision is compatible with our legal obligation. Where there is discrimination, but it is considered not to be unlawful – the objective justification must be recorded |
| | *Stop the policy* |

| | |
|---|---|
| | If there would otherwise be unlawful discrimination or adverse effects that are not justified and cannot be prevented/mitigated |