Ada National College for Digital Skills

Data Protection Policy

Version	Purpose/Changes	Author	Date
1	Policy drafted to incorporate current legislation	Ian Dickerson	January 2022
2	Rights of Individuals Policy, Data Breach Notification Policy and Data Retention Policy now incorporated into this single document.	Ian Dickerson	January 2024

Date Approved:	January 2024
Approved By:	ELT
Executive Lead:	Chris Payne
Document Owner:	Ian Dickerson
Review due:	January 2027

Distribution

This document has been distributed to:

Name	Position	Date	Version
All Ada governing board	N/A		
All Ada staff	Shared	10/02/2024	2
All prospective staff via Ada website	Published	10/02/2024	2

TABLE OF CONTENTS

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), employer partners, students, trustees, parents 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 Laws and in particular its obligations under 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.

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.

DEFINITIONS

College – Ada, National College for Digital Skills and any subsidiaries

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

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 Laws. Examples of Personal Data of which the College is the Controller 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 Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Lead – Ian Dickerson dataprotection@ada.ac.uk 020 3105 0125

Data Protection Officer – Turn IT On dpo@turniton.co.uk 01865 597620 (option 3 - GDPR)

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, and Sweden.

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

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.

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 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 Laws.

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.

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.

COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

All College Personnel must comply with this 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.

College Personnel must not release or disclose any Personal Data:

- outside the College; or
- inside the college to College Personnel not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Lead; this includes by phone calls or in emails.

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.

DATA PROTECTION PRINCIPLES

When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- 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;
- kept for no longer than is necessary for the purposes for which it is being processed; and
- 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.

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

In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. 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.

LAWFUL USE OF PERSONAL DATA

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

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

The College has carefully assessed how it uses Personal Data and how it complies with these obligations. This is documented in the College's Record of Processing Activity. 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 Lead who will decide whether their intended use requires amendments to be made, whether a Privacy Impact Assessment should be carried out, and any other controls which need to apply.

TRANSPARENT PROCESSING – PRIVACY NOTICES

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. The College has adopted the following privacy notices: Privacy Notice - College Staff and Privacy Notice for Students.

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.

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

Data Protection Laws 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 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.

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.

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.

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).

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 Laws. See Rights of Individuals below. 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.

PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

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

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 Retention Schedule.

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 Retention Schedule, 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 Lead for guidance.

DATA BREACHES

WHAT IS A PERSONAL DATA BREACH?

The College takes information security very seriously and 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.

A 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 can also occur as a result of something someone internal does.

A Personal Data breach could include any of the following:

- loss or theft of Personal Data or equipment that stores Personal Data;
- loss or theft of Personal Data or equipment that stores the College's Personal Data from a College supplier;
- inappropriate access controls meaning unauthorised College Personnel can access Personal Data;
- any other unauthorised use of or access to Personal Data;
- deleting Personal Data in error;
- human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);

- hacking attack;
- infection by ransom ware or any other intrusion on our systems/network;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it; or
- destruction or damage to the integrity or accuracy of Personal Data.

A Personal Data breach can also include:

- equipment or system failure that causes Personal Data to be temporarily unavailable;
- unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;
- inability to restore access to Personal Data, either on a temporary or permanent basis; or
- loss of a decryption key where Personal Data has been encrypted because this means the College cannot restore access to the Personal Data.

REPORTING A PERSONAL DATA BREACH

College Personnel must immediately notify any Personal Data breach to the Data Protection Lead, no matter how big or small. This allows the College to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the Individuals affected and to the College.

If College Personnel discover a Personal Data breach outside working hours, College Personnel must notify it to the Data Protection Lead as soon as possible.

College Personnel may be notified by a third party (e.g. a supplier that processes Personal Data on the College's behalf) that they have had a breach that affects College Personal Data. College Personnel must notify this breach to the Data Protection Lead and the College's Data Breach Notification Procedure shall apply to the breach.

MANAGING A PERSONAL DATA BREACH

There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

- Containment and recovery
- Assessment of on-going risk
- Notification

- Evaluation and response

At all stages of this Policy, the Data Protection Lead and managers will consider whether to seek external legal advice.

CONTAINMENT AND RECOVERY

An initial assessment of the Personal Data breach will be carried out by the Data Protection Lead with the guidance of the Data Protection Officer where necessary.

If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the Individuals affected then it will be added to the Data Breach Register and no further action will be taken.

If the Personal Data breach may impact on the rights and freedoms of the Individuals affected then the College will put together and implement a bespoke Personal Data breach plan to address the breach concerned in accordance with the Data Breach Notification Procedure. This will include consideration of:

- whether there are any other people within the College who should be informed of the breach, such as IT team members, to ensure that the breach is contained;
- what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and
- whether it is necessary to contact other third parties such as students, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. All notifications shall be made by the Data Protection Lead.

All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Lead.

The Data Protection Lead is responsible for ensuring that the Data Breach Register is updated.

ASSESSMENT OF ONGOING RISK

As part of the response to a Personal Data breach, once the breach has been contained the College will consider the on-going risks to the College and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the

breach. This will be undertaken in accordance with the Data Breach Notification Procedure.

NOTIFICATION

Under Data Protection Laws, the College may have to notify the ICO and also possibly the Individuals affected about the Personal Data breach.

Any notification will be made by the Data Protection Lead following the Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the College becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of Individuals. It is therefore imperative that College Personnel notify all Personal Data breaches to the College in accordance with the Data Breach Notification Procedure immediately.

Notification of a Personal Data breach must be made to the Individuals affected without undue delay where the breach is likely to result in a high risk to the rights and freedoms of Individuals.

Please note that not all Personal Data breaches are notifiable to the ICO and/or the Individuals affected and the College will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

Where the Personal Data breach relates to a temporary loss of availability of the College's systems, the College does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of Individuals. The College does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of Individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

In the case of complex breaches, the College may need to carry out in-depth investigations. In these circumstances, the College will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

When the College notifies the affected Individuals, it will do so in clear and plain language and in a transparent way. Any notifications to Individuals affected will be done in accordance with the Data Breach Notification Procedure. Any notification to an Individual should include details of the action the College has taken in relation to containing the breach and protecting the Individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

The College may not be required to notify the affected Individuals in certain circumstances as exemptions apply. Any decision whether to notify the Individuals shall be taken in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Lead with the support of Data Protection Officer.

EVALUATION AND RESPONSE

It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the College's response to it and the remedial action taken.

There will be an evaluation after any breach of the causes of the breach and the effectiveness of the College's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Data Breach Register.

Any remedial action such as changes to the College's systems, policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

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 appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

One requirement of GDPR is 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 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.

Any contract where an organisation appoints a Processor must be in writing.

You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

GDPR requires the contract with a Processor to contain the following obligations as a minimum;

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;
- to take appropriate security measures;
- to only 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;
- to assist with subject access/Individuals rights;
- 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 type of Personal Data and categories of Individuals; and
- the obligations and rights of the Controller.

A template Data Processing Agreement is available.

RIGHTS OF INDIVIDUALS

COLLEGE PERSONNEL'S OBLIGATIONS

This Policy sets out the rights that Individuals have over their Personal Data under Data Protection Laws. If a member of the College Personnel receives a request from an Individual to exercise any of the rights set out in this Policy, that member of the College Personnel must:

- inform the Data Protection Lead as soon as possible and, in any event, within 24 hours of receiving the request;
- tell the Data Protection Lead what the request consists of, who has sent the request and provide the Data Protection Lead with a copy of the request;
- not make any attempt to deal with, or respond to, the request without authorisation from the Data Protection Lead.

WHAT RIGHTS DO INDIVIDUALS HAVE OVER THEIR PERSONAL DATA?

Right of access (subject access requests)

Individuals have the right to ask the College to confirm the Personal Data about them that the College is holding, and to have copies of that Personal Data (commonly known as a Subject Access Request or SAR) along with the following information:

- the purposes that the College has their Personal Data for;
- the categories of Personal Data about them that the College has;
- the recipients or categories of recipients that their Personal Data has been or will be disclosed to;
- how long the College will keep their Personal Data;
- that they have the right to request that the College corrects any inaccuracies in their Personal Data or deletes their Personal Data (in certain circumstances, please see below for further information); or restrict the uses the College is making of their Personal Data (in certain circumstances, please see below for further information); or to object to the uses the College is making of their Personal Data (in certain circumstances, please see below for further information);
- that they have the right to complain to the ICO if they are unhappy about how the College has dealt with this request or in general about the way the College is handling their Personal Data;
- where the Personal Data was not collected from them, where the College got it from; and
- the existence of automated decision-making, including profiling (if applicable).

The College is not entitled to charge Individuals for complying with this request. However, if the Individual would like a further copy of the information requested, the College can charge a reasonable fee based on its administrative costs of making the further copy.

There are no formality requirements for making a SAR and it does not have to refer to data protection law, or use the words Subject Access Request or SAR. The College will monitor its incoming communications, including post, email, its website and social media pages to ensure that the College can recognise a SAR when it receives it.

The College is required to respond to a SAR within one month from the date the College receives it. If the SAR is complex or there are multiple requests at once, the College may extend this period by two further months provided that the College tells the Individual who has made the SAR about the delay and the College's reasons for the delay within the first month.

The Data Protection Lead will reach a decision as to the complexity of the SAR and whether the College is entitled to extend the deadline for responding.

Right to rectification

Individuals have the right to ask the College to correct any Personal Data about them that the College is holding that is incorrect. The College is then obliged to correct that Personal Data within one month (or two months if the request is complex).

Where the Individual tells the College their Personal Data is incomplete, the College is obliged to complete it if the Individual asks the College to do so. This may mean adding a supplementary statement to their personal file for example.

If the College has disclosed the Individual's inaccurate Personal Data to any third parties, the College is required to tell the Individual who those third parties are and to inform the third parties of the correction where the College can.

When an Individual asks the College to correct their Personal Data, the College is required to do so and to confirm this in writing to the Individual within one month of them making the request.

Right to erasure (right to be forgotten)

Individuals have the right to ask the College to delete the Personal Data the College has about them in certain circumstances but this right is limited in scope and does not apply to every Individual. The right to be forgotten applies when:

- the Personal Data is no longer necessary for the purpose the College collected it for;
- the Individual withdraws consent and the College has no other legal basis to use their Personal Data;
- the Individual objects to the College's processing and there is no overriding legitimate interest for continuing the processing;
- the Personal Data was unlawfully processed; and/or
- the Personal Data has to be erased to comply with a legal obligation.

If the College has disclosed the Individual's deleted Personal Data to any third parties, the College is required to tell the Individual who those third parties are and to inform the third parties to delete the Personal Data where the College can.

When an Individual asks the College to delete their Personal Data, the College is required to do so and to inform the Individual in writing within one month of them making the request that this has been done.

Right to restrict processing

Individuals have the right to "block" or "suppress" the College's processing of their Personal Data when:

- they contest the accuracy of the Personal Data, for a period enabling the College to verify the accuracy of the Personal Data;
- the processing is unlawful and the Individual opposes the deletion of the Personal Data and requests restriction instead;
- the College no longer needs the Personal Data for the purposes the College collected it for, but the College is required by the Individual to keep the Personal Data for the establishment, exercise or defence of legal claims;
- the Individual has objected to the College's legitimate interests, for a period enabling the College to verify whether its legitimate interests override their interests.

If the College has disclosed the Individual's restricted Personal Data to any third parties, the College is required to tell the Individual who those third parties are and to inform the third parties about the restriction where the College can.

When an Individual asks the College to restrict its processing of their Personal Data, the College is required to do so and to confirm to the Individual in writing within one month of them making the request that this has been done.

Right to data portability

Individuals have the right to obtain from the College a copy of their own Personal Data in a structured, commonly-used and machine-readable format (such as CSV files). The aim of this right is to facilitate the ability of Individuals to move, copy or transmit their Personal Data easily from one IT environment to another.

The right to data portability only applies when:

- the Individual provided the College with the Personal Data;
- the processing the College is carrying out is based on the Individual's consent or is necessary for the performance of a contract; and
- the processing is carried out by automated means.

This means that the right to data portability does not apply to personal data the College is processing on another legal basis, such as its legitimate interests.

The College is obliged to provide this information free of charge within one month of the Individual making the request (or two months where the request is complex provided that the College explains to the Individual why it needs more time).

The Individual also has the right to ask the College to transmit the Personal data directly to another organisation if this is technically possible.

Right to object

Individuals have the right to object to the College's processing of their Personal Data where:

- the College's processing is based on its legitimate interests or the performance of a task in the public interest and the Individual has grounds relating to his or her particular situation on which to object;
- the College is carrying out direct marketing to the Individual; and/or
- the College's processing is for the purpose of scientific/historical research and statistics and the Individual has grounds relating to his or her particular situation on which to object.

If an Individual has grounds to object to the College's legitimate interests, the College must stop processing their Personal Data unless the College has compelling legitimate grounds for the processing which override the interests of the Individual, or where the processing is for the establishment, exercise or defence of legal claims.

If an Individual objects to direct marketing, the College must stop processing their Personal Data for these purposes as soon as the College receives the request. The College cannot refuse their request for any reason and cannot charge them for complying with it.

Before the end of one month from the date the College gets the request, the College must notify the Individual in writing that the College has complied or intends to comply with their objections or that the College is not complying and the reasons why.

Rights in relation to automated decision making

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is:

- necessary for entering into or performing a contract between the College and the Individual;
- required or authorised by Data Protection Laws; or
- based on the Individual's explicit consent.

Automated decision making happens where the College makes a decision about an Individual solely by automated means without any human involvement. Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

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. GDPR brings about a number of important changes for organisations that market to Individuals, including:

- providing more detail in their privacy notices, including for example whether profiling takes place; and
- rules on obtaining consent will be stricter and will require an Individual's "clear affirmative action".

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

Consent is central to electronic marketing. Best practice is to provide an un-ticked opt-in box.

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

- contact details have been obtained in the course of a sale (or negotiations for a sale);
- the College are marketing its own similar services; and
- the College gives the Individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

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.

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 Laws. If College Personnel therefore wish to carry out any Automated Decision Making or Profiling they must inform the Data Protection Lead.

College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Lead.

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

DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The GDPR requires the College 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 which 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
- the measures 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 Data Protection Impact Assessment 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 e.g. CCTV cameras.

All DPIAs must be reviewed and approved by the Data Protection Lead. A template DPIA is available.

TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

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 the College appoints a supplier with group companies outside the EEA which 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 unless it has been approved by the Data Protection Lead.

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