

Data Protection Policy

APPROVED BY EMT: (Principal to sign)	Pat Brennan-Barrett	(Signature)
	Principal	(Position)
	Sept 2019	(Date)
	July 2019	(Review)

TABLE OF CONTENTS

1. OVERVIEW	3
2. ABOUT THIS POLICY	3
3. DEFINITIONS	3
4. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS	5
5. DATA PROTECTION PRINCIPLES.....	5
6. LAWFUL USE OF PERSONAL DATA	6
7. TRANSPARENT PROCESSING – PRIVACY NOTICES	8
8. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA.....	9
9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED	10
10. DATA SECURITY	10
11. DATA BREACH	10
12. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA	12
13. INDIVIDUALS' RIGHTS	13
14. MARKETING AND CONSENT	15
15. AUTOMATED DECISION MAKING AND PROFILING.....	15
16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)	16
17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA.....	17

Please note that explanatory notes and additional guidance are shown in bold, italic fonts

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 students, employees, suppliers (sole traders, partnerships or individuals within companies), governors, 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 Article 5 of 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.

All College Personnel will receive mandatory training and have ready access to this policy through the Document Library, which will be revised periodically. 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 Officer, who is responsible for ensuring the College's compliance with this Policy.

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.

3. DEFINITIONS

- 3.1. **College** – Northampton College
- 3.2. **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.
- 3.3. **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 Laws. 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.

- 3.4. **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.
- 3.5. **Data Protection Officer** – Our Data Protection Officer is Northampton College’s Director of Finance & Corporate Affairs, and can be contacted at: steve.rankine@northamptoncollege.ac.uk
Tel 01604 734380
- 3.6. **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.
- 3.7. **ICO** – the Information Commissioner’s Office, the UK’s data protection regulator.
- 3.8. **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.
- 3.9. **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.

Note: Paragraph 3.9 defines Personal Data. There are two types of Personal Data and it is important to work out which category your Personal Data falls into. There is ordinary Personal Data and Special Categories of Personal Data (previously, “sensitive Personal Data”). Stricter rules apply to the collection and use of Special Categories of Personal Data. The easiest way to work out which category your Personal Data falls into is to consider whether it is Special Categories of Personal Data first as there is a defined list of this type of Personal Data. Ordinary Personal Data is everything else.

- 3.10. **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.

- 3.11. **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.

4. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

- 4.1. All College Personnel must comply with this policy.
- 4.2. 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.
- 4.3. College Personnel must not release or disclose any Personal Data:
 - 4.3.1. outside the College; or
 - 4.3.2. 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.
- 4.4. 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.

5. DATA PROTECTION PRINCIPLES

- 5.1. When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:
 - 5.1.1. processed lawfully, fairly and in a transparent manner;
 - 5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - 5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
 - 5.1.4. 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;
 - 5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and
 - 5.1.6. 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.
- 5.2. These principles are considered in more detail in the remainder of this Policy.

- 5.3. 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.

Accountability requires compliance with the GDPR to be documented. It is not enough to comply; you have to be able to demonstrate that you are complying through documentation. Colleges must therefore put together written policies and procedures that document compliance. An example of a policy includes this Policy, but we have also set out examples of additional policies that the College should consider putting in place:

- *Data retention – which details how long you hold personal data for;*
- *Policies that implement individuals rights, including subject access requests; and*
- *Data breach reporting.*

In addition, the College should ensure that the results of any data audit carried out and decisions made in relation to data protection issues are recorded.

6. LAWFUL USE OF PERSONAL DATA

Note: It is essential that the collection and use of Personal Data is lawful. This means that any use of the Personal Data must fall within one of a number of gateways or "lawful purposes".

The College needs to assess which lawful purpose applies to make each use of Personal Data lawful. This paragraph 6 sets out that the College has assessed how it uses its Personal Data and that it complies with at least one of the lawful purposes. If the use changes then the assessment will need to be redone. The use of Personal Data should be reviewed periodically and any initial data audit updated periodically too. The analysis should not stop on 25th May. No GDPR compliance programme should be seen as "set in stone" as the uses of Personal Data will change.

Lawful purposes for processing ordinary Personal Data

These are set out in Article 6 of the GDPR and are as follows (paraphrased):

- *the use of the Personal Data is for the purposes of the legitimate interests of the Controller;*
- *the processing is necessary for the performance of a contract;*
- *the processing is necessary for compliance with a legal obligation;*
- *the processing is necessary in order to protect the vital interests of the individual or of another natural person;*
- *the processing is necessary for the performance of a task carried out in the public interest; and*
- *the individual who is the subject of the Personal Data has given consent for one or more specific purposes.*

Where a College is a public body, it cannot rely on the lawful purpose of legitimate interests where the processing is in the performance of a task carried out in the public interest or in

the exercise of official authority. Instead, it needs to rely on the processing being necessary for the performance of a task carried out in the public interest.

Using consent to make your use of ordinary Personal Data lawful:

Before relying on consent as the gateway for legitimising any processing, you should note that there are strict requirements on how it can be used (consent needs to be specific, freely given and informed). Consent can also be withdrawn at any time meaning that the Personal Data can no longer be processed.

In addition, in terms of the College's relationships with its employees, ICO guidance has stated that consent is not available in an employer and an employee relationship. The reasoning behind this is that the relationship is imbalanced and so the employee cannot really refuse to give their consent. Similarly, the ICO has commented that, for similar reasons, public authorities such as Colleges will find it difficult to rely on their position of power (e.g. over students).

The College needs to ensure that for each type of ordinary Personal Data it processes, it has established one of the above legal bases for processing it.

Lawful purposes for Special Categories of Personal Data

There are additional conditions which need to be met in order to use Special Categories of Personal Data. These are set out in Article 9 and are as follows (paraphrased):

- *explicit consent;*
- *employment and social security obligations;*
- *vital interests;*
- *necessary for establishment or defence of legal claims;*
- *substantial public interest; and*
- *various scientific and medical issues.*

The College needs to ensure that for each type of Special Categories of Personal Data it processes, it has established one of the above legal bases for processing it.

- 6.1. 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>

- 6.2. 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>

- 6.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. 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.

7. TRANSPARENT PROCESSING – PRIVACY NOTICES

Note:

Colleges must be transparent with individuals about how they will use their Personal Data. This is generally done through a privacy notice. It is mandatory to give more detail in these documents under GDPR than was the case under old data protection legislation and so any existing policies and notices will need to be revamped in readiness for GDPR.

Please refer to the accompanying template privacy notices as starting points for the development of your own privacy notices. Each individual College's notice needs to reflect how that College is processing data – one size does not fit all. Each College will therefore need to tailor the template privacy notices to its own specific circumstances, practices and issues.

The information that needs to be provided is set out in Article 13 and 14 of GDPR. This information comprises (paraphrased):

- *the identity and the contact details of the Controller;*
- *the contact details of the Data Protection Officer, where applicable;*
- *the purposes the Personal Data will be used for as well as the legal basis for the processing;*
- *if legitimate interests is used as a lawful purpose, the legitimate interest must be specified;*
- *the recipients/categories of recipients of the Personal Data, if any;*
- *details of data export and the safeguards applied;*
- *the period the Personal Data will be stored;*
- *the right to request access to, rectification or erasure of Personal Data;*
- *the right to request restriction of use of the Personal Data, the right to object to use as well as the right to data portability;*
- *where the individual has given consent, the right to withdraw that consent;*
- *the right to lodge a complaint with the ICO;*
- *the existence of automated decision making including profiling, the logic involved, as well as the significance and envisaged consequences;*
- *whether the provision of the data is a statutory or contractual obligation and of the possible consequences of failure to provide such data; and*
- *if the Controller intends to further process the Personal Data, provide the individual with information on such further processing.*

Where the Personal Data has not been obtained from the individual who is the subject of the data, the individual must be provided with the information set out above and details of where the Personal Data came from.

The information must be concise and provided in an easy to understand and accessible way in clear and plain language tailored for its specific audience. It is a challenge to provide the required information in a concise way and things such as layering (i.e. providing a short form notice with a link to a longer one) should be adopted. Privacy notices should be issued to staff, students and external parties (e.g. suppliers).

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:

- Students enrolled at any course at the College (including subcontracted courses)
 - Potential students applying or enquiring about courses at the College
- 7.1. 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.
- 7.2. 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.

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

- 8.1. 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 (see paragraph 7 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.

Note:

Paragraph 8.2 discusses the accuracy and relevance of Personal Data.

Accuracy and Relevance of Personal Data:

The College needs to understand the purpose for which Personal Data has been collected and is being used and must ensure that irrelevant Personal Data is not collected. This is known as data minimisation. Personal Data must not be collected "just in case" and forms that are used to collect data should be reviewed to determine whether any sections can be made optional.

Personal Data must be accurate. Formal practices should be put in place dealing with data accuracy. Common problems which arise in this area are where there are multiple systems which capture the same information, but do not talk to each other meaning updates to the information are not always picked up.

Checks should be carried out on a regular basis to ensure that the data held is accurate. If the data is inaccurate or has changed, processes should be put in place to make sure that it is erased or rectified.

- 8.2. 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.
- 8.3. 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.

- 8.4. 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).
- 8.5. 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 Laws. 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.

9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

Please refer to the accompanying Data Retention Policy.

- 9.1. 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.
- 9.2. 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.
- 9.3. 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.

10. DATA SECURITY

It is a requirement of GDPR that appropriate technical and organisational security measures are used, monitored, controlled and audited to protect against unauthorised processing, accidental loss, destruction or damage of Personal Data.

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.

11. DATA BREACH

Please refer to the accompanying Data Breach Notification Procedure.

What happens if the College is subject to a data breach?

Under the GDPR, College's will be obliged to notify the ICO in the event of a Data Breach unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Notification must take place within 72 hours of the College becoming aware of the breach.

You will also be obliged to notify the individuals affected by the Data Breach as soon as possible where the breach is likely to result in a high risk to their rights and freedoms, for example identity theft or fraud or where the breach may give rise to discrimination. If you are in doubt as to whether a data breach is reportable then the ICO has set up a hotline which will give guidance on this.

You will not be obliged to notify the individuals affected where:

- there are technological and organisational protection measures (e.g. encryption);*
- the Controller has taken action to eliminate the high risk; and*
- it would involve disproportionate effort – in this case they must be informed some other way e.g. by a notice in newspapers.*

You will still have to notify the ICO.

When do you become aware of a data breach?

You are only aware of a data breach once you have a reasonable degree of certainty that there has been a security incident and Personal Data has been compromised. This means that it is possible for you to carry out a short investigation to establish whether there is a breach and the ability to do this needs to be factored into data breach planning.

The practicalities of dealing with a data breach

In view of the short timescale for reporting the data breach, it is important, as part of GDPR compliance, to plan for a data breach and consider matters such as how a data breach may occur, what impact it may have and how it may be rectified.

Even if it is decided that a data breach is not notifiable, all data breaches must be documented on an internal data breach register and this is something which all Colleges will need to put in place. It is also important in managing the risk relating to data breach that there is a culture of encouraging disclosure through an internal reporting process.

Training

All individuals who have access to Personal Data should be appropriately trained in data protection. This should be done at a level suitable for their job roles and the interaction they will have with Personal Data. Training is important to reduce the likelihood of misuse of Personal Data and the nature and frequency of the training is also taken into consideration by the ICO in considering the appropriate sanction in the event of a breach. Training should be provided to staff that is planned, timetabled and regular. Documentation should be put together which tracks who has been trained, on what and on what date.

- 11.1. 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 there will be a Personal Data breach and College Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 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.

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

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

11.3.1. **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;

11.3.2. **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

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

12. **APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA**

12.1. 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.

12.2. 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.

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

12.4. 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.

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

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

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

- 12.5.3. to ensure staff are subject to confidentiality obligations;
- 12.5.4. to take appropriate security measures;
- 12.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- 12.5.6. to keep the Personal Data secure and assist the Controller to do so;
- 12.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- 12.5.8. to assist with subject access/individuals rights;
- 12.5.9. to delete/return all Personal Data as requested at the end of the contract;
- 12.5.10. to submit to audits and provide information about the processing; and
- 12.5.11. to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

12.6. In addition the contract should set out:

- 12.6.1. The subject-matter and duration of the processing;
- 12.6.2. the nature and purpose of the processing;
- 12.6.3. the type of Personal Data and categories of individuals; and
- 12.6.4. the obligations and rights of the Controller.

Note:

*Please refer to the accompanying **GDPR Contract Variation Agreement** with GDPR – compliant data processing clauses for standard form provisions to incorporate these points.*

These provisions are stricter than what has gone before. Existing arrangements will need to be varied to include these new clauses and new arrangements will need to include them. A related issue is that of liability. On the basis that the potential fines for GDPR breach are much higher than for breach of old data protection legislation you should look at liability clauses in your processor contracts and consider whether liability is capped at too low an amount.

13. INDIVIDUALS' RIGHTS

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

- 13.1. GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that Colleges plan how they will handle these requests under GDPR.
- 13.2. The different types of rights of individuals are reflected in this paragraph.

13.3. **Subject Access Requests**

13.3.1. Individuals have the right under the 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 extension if it is a complex request). In addition, you will no longer be able to charge a fee for complying with the request.

13.3.2. 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.

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

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

- 13.4.1.1. the use of the Personal Data is no longer necessary;
- 13.4.1.2. their consent is withdrawn and there is no other legal ground for the processing;
- 13.4.1.3. the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- 13.4.1.4. the Personal Data has been unlawfully processed; and
- 13.4.1.5. the Personal Data has to be erased for compliance with a legal obligation.

13.4.2. 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.

13.5. **Right of Data Portability**

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

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

13.5.2. This right isn't the same as subject access and is intended to give individuals a subset of their data.

13.6. **The Right of Rectification and Restriction**

13.6.1. Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

13.7. 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 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.

14. MARKETING AND CONSENT

- 14.1. The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.
- 14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR will bring about a number of important changes for organisations that market to individuals, including:
 - 14.2.1. providing more detail in their privacy notices, including for example whether profiling takes place; and
 - 14.2.2. rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.
- 14.3. Colleges also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply 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
- 14.4. Consent is central to electronic marketing. We would recommend that best practice is to provide an un-ticked opt-in box.
- 14.5. Alternatively, the College may be able to market using a "soft opt in" if the following conditions were met:
 - 14.5.1. contact details have been obtained in the course of a sale (or negotiations for a sale);
 - 14.5.2. the College are marketing its own similar services; and
 - 14.5.3. 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.

15. AUTOMATED DECISION MAKING AND PROFILING

Note: GDPR highlights profiling and automated decision making as two areas of particular concern and imposes additional controls in relation to them. Profiling and automated decision making are two different things although automated decision making can include profiling.

Profiling occurs if there is any element of automation in analysing or predicting behaviours or preferences (e.g. staff utilisation reports, analysis of performance at work). Profiling can therefore happen even if the ultimate decision is not taken by a machine. If there is profiling then obligations under the GDPR relating to transparency, data accuracy, data minimisation and retention must be carefully thought about.

Automated decision making is a step further where a decision is made based solely on automated processing which produces legal effects in relation to an individual or similarly significantly affects the individual.

Colleges need to consider very carefully whether any current processing operations carry out profiling or automated decision making.

- 15.1. 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.

- 15.2. 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 College Personnel must inform the Data Protection Officer.
- 15.3. College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.
- 15.4. The College does not carry out Automated Decision Making or Profiling in relation to its employees.

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

- 16.1. The GDPR introduce 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 which need to be considered before a new product/service/process is rolled out. The process is designed to:

- 16.1.1. describe the collection and use of Personal Data;

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

- 16.1.3. assess the risks to the rights and freedoms of individuals; and

- 16.1.4. the measures to address the risks.

- 16.2. 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.

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

- 16.4. 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.
- 16.5. 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):
 - 16.5.1. 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;
 - 16.5.2. 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
 - 16.5.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.
- 16.6. All DPIAs must be reviewed and approved by the Data Protection Officer.

17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

- 17.1. 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.
- 17.2. 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 Officer.
- 17.3. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.