Bolton College

Data Protection Policy

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....6
8. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA....6
9. DATA RETENTION....7
10. DATA SECURITY....7
11. DATA BREACH....7
12. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA....8
13. COLLEGE PERSONNEL'S OBLIGATIONS REGARDING DATA REQUESTS....9
14. INDIVIDUALS' RIGHTS....10
15. MARKETING AND CONSENT....12
16. AUTOMATED DECISION MAKING AND PROFILING....13
17. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)....13
18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK....14

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 relating to individuals and organisations including employees, students, suppliers, visitors and others. 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.

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 staff will be signposted to a copy of this Policy when they start and may receive notifications of revisions. 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) set out the basis on which the College will collect and use Personal Data either where the College collects it from individuals directly, 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.

The legal responsibility for compliance with Data Protection Law lies with the College who is the 'data controller', registered as such with the Information Commissioner's Office. Responsibility for compliance is delegated to College Managers who are responsible for encouraging data processing best practice within the College. However, compliance with this policy is the responsibility of everyone within the College who processes personal information.

3. DEFINITIONS

3.1. **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**.**

3.2. **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.

3.3. **Data Protection Laws** – The Data Protection Act 2018 sets out the framework for data protection law in the UK. It came into effect on 25 May 2018 and was subsequently amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU. It sits alongside and supplements the UK GDPR which is a UK law which came into effect on 01 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, with some changes to make it work more effectively in a UK context. Where any overseas data was collected before 01 January 2021 (referred to as 'legacy data'), this will be subject to the EU GDPR as it stood on 31 December 2020 (known as 'frozen GDPR'). The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

3.4. **Data Protection Officer** – The College Data Protection Officer can be contacted at: 01204 482020 or dpo**.**boltoncc.ac.uk. The DPO may delegate responsibility to a member of the Senior Management Team or other College Managers where appropriate.

3.5. **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.

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

3.7. **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.

3.8. **PECR - The Privacy and Electronic Communications Regulations** sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.

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.

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:

- 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 Officer; this includes by phone calls or in emails. A separate document 'Disclosing information outside the College' provides guidance on dealing with requests from third parties.

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:

- 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.

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.

6. LAWFUL USE OF PERSONAL DATA

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. These are documented in the Data Use and Retention Schedule

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. Where possible we will try to obtain your explicit consent, unless it is a requirement of our statutory duty.

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

7.1. 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. The College has adopted the following privacy notices:

- Bolton College Privacy Notice for Staff
- Bolton College Privacy Notice for Students
- Bolton College General Privacy Notice
- Bolton College Privacy Notice for Visitors to our Website

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.

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. 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 the appropriate section within this document.

9. DATA RETENTION

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 Use and Retention Schedule.

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 Use and 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

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

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:

- **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;

- **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

- **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 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.

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. UK 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 UK Data Protection Law.

12.6. 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.

13. COLLEGE PERSONNEL'S OBLIGATIONS REGARDING DATA REQUESTS

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

13.2. UK 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 UK GDPR.

13.3. The different types of rights of individuals are reflected in the next section.

14. INDIVIDUALS' RIGHTS

14.1. Subject Access Requests

14.1.1. 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 extension if it is a complex request). In addition, the College is no longer able to charge a fee for complying with the 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.

14.1.2. 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.

14.1.3. The College has supplied a template Subject Access Request (SAR) form which is available on the College website and intranet. However, there are no formality requirements to making a SAR and it does not have to refer to data protection law, or use the words Subject Access Request or SAR.

14.1.4. 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.

14.1.5. 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.

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

14.2. Right of Erasure (Right to be Forgotten)

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

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

14.2.2. 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.

14.2.3. 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.

14.2.4. 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.

14.3. **Right of Data Portability**

14.3.1. 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:

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

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

14.3.3. This right is 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.

14.3.4. 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.

14.3.5. 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).

14.3.6. The individual also has the right to ask the College to transmit the Personal data directly to another organisation if this is technically possible. Such requests must be in writing.

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

14.4.1. 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.

14.4.2. 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).

14.4.3. 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.

14.4.4. 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.

14.4.5. 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.

15. MARKETING AND CONSENT

15.1. 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.

15.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals or organisations. UK GDPR includes strict rules on obtaining consent and will require an individual's "clear affirmative action". Consent is central to electronic marketing and best practice is to provide an un-ticked opt-in box.

15.3. Alternatively, the College may be able to market using a "soft opt in" if the following conditions are 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.

15.4. College Personal also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR give specific privacy rights in relation to electronic communications. There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

PECR rules use the UK GDPR standard of consent. This means that if you send electronic marketing or use cookies or similar technologies you must comply with both PECR and the UK GDPR.

It is important to understand that PECR apply even if you are not processing personal data. For example, many of the rules protect companies as well as individuals, and the marketing rules apply even if you cannot identify the person you are contacting.

The ICO has several ways of taking action to change the behaviour of anyone who breaches PECR. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner can also serve a monetary penalty notice imposing a fine of up to £500,000 which can be issued against the organisation or its directors. These powers are not mutually exclusive.

For more information on PECR go to https://icosearch.ico.org.uk/s/search.html?query=pecr&collection=ico-meta&profile=_default

16. AUTOMATED DECISION MAKING AND PROFILING

16.1. 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.

16.2. 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.

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

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

17. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

17.1. The UK GDPR includes a 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:

- 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.

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 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.

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):

- 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.

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

18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

18.1. Individuals risk losing the protection of the UK data protection laws if their personal data is transferred outside of the UK. On that basis, the UK GDPR restricts transfers of personal data to a separate organisation located outside of the UK, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.

18.2. Following the UK leaving the EU, there remains provision that permits the transfer of personal data from UK to the EEA and to any countries which, as at 31 December 2020, were covered by a European Commission 'adequacy decision'. This is to be kept under review by the UK Government.

18.3. Transfer includes sending Personal Data outside the UK but also includes storage of Personal Data or access to it outside the UK. This MUST be considered whenever the College appoints a supplier outside the UK or the College appoints a supplier with group companies outside the UK which may give access to the Personal Data to staff outside the UK.

18.4. So that the College can ensure it is compliant with Data Protection Laws College Personnel must not agree arrangements to transfer Personal Data unless it has been approved by the Data Protection Officer.

Updated By: Tracy Clarke (Director of MIS and Curriculum Development)
Last Updated Date: January 2022
Version: DP1/2022
Next Review Date: January 2024