Richmond upon Thames College

Policy Name:	General Data Protection Policy
Policy Number/Version No:	Version 3
Effective Date:	August 2022
Review Date:	No later than 31st August 2023
Policy Responsibility:	Data Protection Officer
Approved By:	Audit Committee / Corporation

Table of Contents

1. OVERVIEW

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

Richmond Upon Thames College collects, uses and stores Personal Data about its students, applicants, alumni, 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 the General Data Protection Regulation (Regulation (EU) 2016/679) (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.

This Policy will be made available to all College Personnel. It does not form part of any 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. Non-compliance may result in disciplinary action.

If you have any queries concerning this Policy, please contact the 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

College – Richmond Upon Thames College

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 decides 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.

Criminal records data – means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data Protection Laws – UK General Data Protection Regulations are governed by the Data Protection Act 2018. Further information regarding the transition from EU law is available at https://www.gov.uk/guidance/using-personal-data-in-your-business-or-other-organisation-after-the-transition-period

Data Protection Officer – Our Data Protection Officer is Alison de Lord and can be contacted on Teams or by email alison.de.lord@rutc.ac.uk.

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

Individuals / natural person – Living individuals who can be identified, *directly or indirectly*, from information that the College holds. 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, potential students and alumni. 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 email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address, photographs and video footage including CCTV images and also more sensitive types of data which are defined below.

Processing
Processing covers almost anything which is done with or to the data, including:

- recording, or entering data onto files;
- holding data, or keeping it on file, without doing anything to it or with it;
- organising, altering or adapting data in any way;
- retrieving, consulting or otherwise using data;
- disclosing data either by giving it out, by sending it on e-mail, or simply by making it available;
- combining data with other information;
- erasing or destroying data.

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

A Processor can be 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.

4. GENERAL OBLIGATIONS OF COLLEGE PERSONNEL

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, 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.

5. 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.

6. 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, which are defined by the ICO as follows.

(a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. Relevant provisions in the GDPR - See Article 6 and Recitals 39, 40, and Chapter III (Rights of the data subject) External link 02 August 2018 - 1.0.248 4

(c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

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 (all quotations taken from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/):

i. **Explicit consent**, where "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes"

ii. **Employment, social security and social protection law**, if: "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject"

iii. **Vital interests**, if: "processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent", or "where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person…"

iv. **Not-for-profit bodies**, if: "processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects"

v. **Made public by the data subject**, if: "processing relates to personal data which are manifestly made public by the data subject"

vi. **Legal claims and judicial acts**, if: "processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity"

vii. **Substantial public interest**, if: "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"

viii. **Health or social care**, if: "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3"

ix. **Public health**, if: "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy"

x. **Archiving, research and statistics**, if: "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject"

The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out above. If the College changes how it uses Personal Data, the College will 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

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. This information comprises:

- 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 kept;
- 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. Layering (i.e. providing a short form notice with a link to a longer one) can be adopted. Privacy notices should be issued to staff, students and external parties (e.g. suppliers).

College has adopted privacy statements, as provided on the College website.

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.

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 the Data Protection Officer should be notified who will then 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

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.

All College Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately and is kept up to date. They 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. 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

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 Data Retention Policy.

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

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

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 Policy. College Personnel should alert the Data Protection Officer to a data breach in the first instance as soon as the breach has been identified.

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.

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

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 and data sharing agreements 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.

The College is considered as having appointed a Processor where it has engaged someone or a company to perform a service for the College and as part of it would have access to Personal Data. Where you appoint a Processor, the 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.

13. INDIVIDUALS' RIGHTS

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

Subject Access Requests

Individuals have the right under the GDPR to ask the 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, it is no longer possible to charge a fee for complying with the request.

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.

Right of Erasure (Right to be Forgotten)

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.

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.

Right of Data Portability

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

This right is not the same as subject access and is intended to give individuals a subset of their data.

The Right of Rectification and Restriction

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.

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. College personnel need to familiarise themselves 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. INDIVIDUAL RESPONSIBILITIES

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the College know if data provided to the organisation changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and of our students and other stakeholders in the course of their employment, contract, volunteer period or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to our students and other stakeholders.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

- not to remove personal data, or devices containing or that can be used to access personal data, from the College's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the Data Protection Officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the College's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

15. 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 will bring 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". The ICO like consent to be used in a marketing context.

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

Consent is central to electronic marketing. We would recommend that 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 opt out of the marketing, both when first collecting the details and in every message after that.

16. 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 College Personnel must inform the Data Protection Officer.

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

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

17. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

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

18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE UK

Data Protection Laws impose strict controls on Personal Data being transferred outside the UK. Transfer includes sending Personal Data outside the UK but also includes storage of Personal Data or access to it outside the UK. It needs to be thought about 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. College Personnel must not export any Personal Data outside the UK without the approval of the Data Protection Officer. The approval will depend on the degree to which country complies with data protection requirements similar to that of UK GDPR such as the Data Shield in the US.

For EU/EEA considerations, The EU-UK Trade and Cooperation Agreement contains a bridging mechanism that allows the continued free flow of personal data from the EU/EEA to the UK after the transition period until adequacy decisions come into effect, for up to 6 months. EU adequacy decisions for the UK would allow for the ongoing free flow of data from the EEA to the UK.