GENERAL DATA PROTECTION POLICY

Policy Reference:	POL-356
Policy Area:	Data Protection
Policy Owner:	Stephen Belling
Policy Author:	Lisa Hutchinson
Level of Consultation:	Level 1
Approval Level:	SLT
Review Date:	March 2025
Approval Date:	May 2025
Next Approval Date:	March 2027

TABLE OF CONTENTS

1. OVERVIEW

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

As an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, 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 UK GDPR.

The College has implemented this Data Protection Policy to ensure all College Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

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

If you have any queries concerning this Policy, please contact our Data Protection 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 – Birmingham Metropolitan 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 UK GDPR 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 can be contacted at: 0121 446 4545 or alternatively email dpo@bmet.ac.uk.

3.6. **UK GDPR** – The General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

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.

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.

3.12. **UK Adequacy Regulations** – the legal framework in that country, territory, sector or international organisation has been assessed as providing 'adequate' protection for individuals' rights and freedoms for their 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 not misuse Personal Data. For example, accessing Personal Data not for the purpose of carrying out their College role.

4.5. College Personnel must take all steps to ensure there is no unauthorised access to, or authorised access misuse of 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.

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 under Article 6 of the UK GDPR. Please click here to see the detailed grounds [A guide to lawful basis | ICO]

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 under Article 9 of the UK GDPR. Please click here to see the detailed additional conditions [Special category data | ICO].

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 privacy notices which are available on the College SharePoint pages, and on the BMet corporate website for external audiences (Privacy Notice - About BMet - Birmingham Metropolitan College).

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

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

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. The College has separate protocols which set out how the College responds to requests relating to these issues and these are available on Sharepoint. 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

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 and Disposal 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 and Disposal 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 Protocol. Please see 'What is a Data Breach?' and 'Examples of reportable data breaches and near misses' 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, access to or misuse of Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data not for the purpose of carrying out their College role, 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 person, 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 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:

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 and appropriately trained to handle and process the Shared Personal Data in accordance with technical and organisational security measures together with any other applicable data protection laws and guidance;

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 complying with subject individual rights including access to and rectification of personal data;

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

12.5.10. to regularly review the agreement and how these reviews will be conducted;

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

12.5.12. to tell the Controller if any instruction is in breach of Data Protection Laws.

12.6. In addition the contract should set out:

12.6.1. The purpose, subject-matter and duration of the processing;

12.6.2. the nature and legal justification of the processing;

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

12.6.4. the existence of and conditions under which any special category data is being shared; and

12.6.5. the obligations and rights of the Controller.

13. INDIVIDUALS' RIGHTS

13.1. 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.

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

13.3. **Right to be Informed**

13.3.1. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR and how the College complies with this is detailed in section 7 of this policy.

13.4. **Right of Access / Subject Access Requests**

13.4.1. Individuals have the right under the UK GDPR to ask a College to confirm what Personal Data they hold in relation to them and provide them with the data. The timescale for providing this data is without undue delay and at least within one calendar month of receiving the request. In exceptional cases where the DPO has concluded that a request is complex or if we have received a number of requests from the individual, the time limit may be extended by a further two months.

13.4.2. If a large amount of information about an individual is processed, the DPO may ask the individual to specify the information or processing activities their request relates to before responding. The time limit for responding to the request is paused until clarification is received. This is referred to as 'stopping the clock'. Clarification will only be sought if it is genuinely required in order to respond to a SAR and if a large amount of information about the individual is processed.

13.4.3. In cases where the identity of the individual is not obvious it will be necessary for the DPO to take reasonable and proportionate steps to verify the identity of the individual. In instances where the identity of the individual requires verification a request will be made to compete the college Subject Access Request Form with appropriate supporting evidence. As with 13.4.2 time limit for responding to the request is paused until clarification is received ('stopping the clock') and will not restart until which point the individual's identity has been verified.

13.4.4. In most cases we are unable to charge a fee to comply with a request. A reasonable fee for the administrative costs of complying with a request may only be charged in instances where the request is assessed and adjudged to be manifestly unfounded or excessive, or if an individual requests further copies of their data.

13.4.5. 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 and escalated to the DPO without delay to avoid a complaint being made to the ICO.

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

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

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

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

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

13.5.1.4. the Personal Data has been unlawfully processed; and

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

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

13.5.3. In cases where the identity of the individual is not obvious it will be necessary for the DPO to take reasonable and proportionate steps to verify the identity of the individual. In instances where the identity of the individual requires verification a request will be made to compete the college Erasure Request Form with appropriate supporting evidence. The DPO must inform the individual without undue delay and within one month that more information is required to confirm their identity. The college does not need to comply with the request until the additional information has been received.

13.6. **Right of Data Portability**

13.6.1. 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:

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

13.6.1.2. the processing is carried out by automated means

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

13.7. **The Right of Rectification, Restriction and Objection**

13.7.1. 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 including until inaccuracies in their data are rectified.

13.7.2. The individual has the right to object to the processing of personal data that is carried out in the public interest, exercise of official authority vested in the college or legitimate interests. In these circumstances the right to object is not absolute and processing may continue where the College can justify the grounds on which the processing takes place.

13.7.3. An individual can object to the processing of their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

13.8. 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 various protocols.

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. UK GDPR introduced 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".

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

14.4. Alternatively, the College may be able to market using a "soft opt in" if the following conditions are met. The advice of the Data Protection Officer should be sought if the following conditions are met:

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

14.4.2. the College are marketing its own similar services; and

14.4.3. 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

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 UK GDPR has 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:

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 College's protocol is available on Sharepoint.

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. RECORDS OF PROCESSING ACTIVITY (INFORMATION ASSET REGISTER)

17.1. The UK GDPR has a requirement to maintain a Record of Processing Activities ("ROPA"). The College will maintain a ROPA which includes the minimum requirements of:

17.1.1. College name and contact details, whether the processing activity is as a Controller or a Processor (and where applicable, the Joint Controller, and their representative DPO;

17.1.2. The purpose of the processing;

17.1.3. A description of the categories of individuals and of personal data;

17.1.4. The categories of recipients of personal data;

17.1.5. Details of transfers to third countries, including a record of the transfer mechanism safeguards in place;

17.1.6. Retention schedules, and

17.1.7. A description of the technical and organisational security measures in place

17.2. In addition to the minimum requirements the College ROPA will also include:

17.2.1. Details of Information Asset Owners, and

17.2.2. Contract and/or Data Sharing Agreement numbers, where applicable.

17.3. All Personal Data, electronic or paper data files, retained by the College must be recorded on the Information Asset Register. The Information Asset Owner (IAO) must provide the DPO with the necessary information to ensure compliance with the College's Data Protection Policy.

17.4. The IAO role is to

17.4.1. understand what information is held within their Department;

17.4.2. How it is used;

17.4.3. Who has access to it and why;

17.5. The IAO responsibilities include:

17.5.1. To promote a culture that values and protects College information

17.5.2. Know what information is held, what enters and leaves it, and why

17.5.3. Know who has access and why, and ensure their use of the information is monitored

17.5.4. Understand and address risks to the information and provide assurance to the DPO

17.5.5. Ensure appropriate use of the information

17.6. A review of the Data Processing Activity must be undertaken by the IAO at least every twelve months

17.7. Updates or changes to the Data Processing Activity must be notified by the IAO to the DPO.

17.8. The DPO must undertake a full review of the ROPA at least every twelve months.

18. TRANSFERRING PERSONAL DATA OUTSIDE OF THE UK

18.1. The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations. These restrictions apply to all transfers, no matter the size of transfer or how often they are carried out. Transfer includes sending Personal Data outside the UK or to a territory not covered by UK adequacy regulations but also includes storage of Personal Data or access to it outside the of these regions. It needs to be considered whenever the College appoints a supplier outside this remit or the College appoints a supplier with group companies not covered by UK adequacy regulations and which may give access to the Personal Data to staff not covered by UK adequacy regulations.

18.2. 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.

18.3. College Personnel must not export any Personal Data outside the UK or to a territory that isn't covered by UK adequacy regulations without the approval of the Data Protection Officer.