BSix Brooke House Sixth Form College Policy Document

General Data Protection Policy

Subject:	Data protection including GDPR
Date of Approval:	May 2019
Effective Date:	May 2019
Review Date:	May 2021
Person Responsible:	Vice Principal Finance & Resources
Approved By:	Board of Corporation
For Action By:	All Staff, Students and Stakeholders
For Information To:	All Staff, Students and Stakeholders

TABLE OF CONTENTS

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

1. OVERVIEW

The BSix Brooke House Sixth Form College needs to collect, store and process personal data in order to carry out its functions and activities as a college. There are many reasons why we need to collect information including Safeguarding, for Health and Safety, to draw down funding for learners, to take fee payments or pay bursaries, or monitoring learning activity are just a few of these reasons. However all staff members within the BSix Brooke House Sixth Form College are committed to protecting the confidentiality and integrity of the personal information it collects in line with the new GDPR legislation.

Under data protection law we have to provide details of how our organisation handles personal data about staff or customers, for the data protection register.

As an organisation that collects, uses and stores Personal Data about its employees, learners, suppliers, partners, governors, parents and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The College has implemented this Data Protection Policy to ensure all College Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

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** – BSix Brooke House Sixth Form College, Kenninghall Road, Hackney, London. E5 8BP.

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, subcontractors, agency staff or temporary staff 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.

The College acts as Controller in relation to areas such as the collection of employee details or enrolment information collected for its learners. It is the organisation itself which is the Controller not the staff.

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

3.5. **Data Protection Officer –** Our Data Protection Officer is Adrian Cottrell and can be contacted via email at acottrell@bsix.ac.uk

3.6. **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

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

3.8. **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include our partners and employers.

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, health data, 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. College examples include, software support we receive for our college student record system, which contains Personal Data, and our outsourced work placement service where we define the purpose and the processing requirements involved.

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 (including learning difficulties or disabilities), sexual life or sexual orientation and criminal convictions. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

4. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

4.1. All College Personnel must comply with this policy.

4.2. College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.3. College Personnel must not release or disclose any Personal Data:

4.3.1. outside the College; or

4.3.2. inside the college to College Personnel not authorised to access the Personal Data,

without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

4.4. College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College.

5. DATA PROTECTION PRINCIPLES

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

5.1.1. processed lawfully, fairly and in a transparent manner;

5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

5.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;

5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and

5.1.6. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

5.3. In addition to complying with the above requirements the College can demonstrate its accountability in adhering to data protection regulations through the other controls it has in place including, but not limited to, its Retention and Destruction Procedure, Data Breach Procedure, Data Rights Procedure, and its Privacy Notice for learners, staff, 14-16 parents and employers.

5.4. The college undertook a scoping exercise and data protection audit as a result of new GDPR legislation to ensure all information and processes were recorded, and processing scaled back to only include what was required. The college will continue to review and develop its compliance under GDPR and will complete in-year audits to monitor internal processes.

6. LAWFUL USE OF PERSONAL DATA

The college lawfully processes Personal Data under the legal basis set out in Article 6 of the GDPR. The majority of processing by the college is done because it is **necessary for the performance of the tasks carried out in the Public Interest.** We limit the information we collect to ensure we only collect what is needed to perform this duty effectively and without penalty. The College also seeks to obtain the **consent from individuals for the purpose of college activities,** either where explicit consent is required (where it is specific, freely given and informed) or where we consider it important that the individual is made aware of the processing even if consent is not required. Our Privacy notices form part of our new learner enrolment process and the new employee induction process and is designed to ensure all learners, staff and parents of children are fully informed of how their data will be used.

Every information asset containing **Ordinary personal data** held by the college has been detailed in our **Record of Processing Activities**. This register details the lawful basis for the collection and processing of all the information we hold. For more information on the lawful basis used for processing please click on the following link [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing]

Additional conditions are imposed on the college where it uses **Special Categories of Personal Data** *(as detailed in Article 9)***.** All **Special Category data** the collect collects is also detailed in the **Record of Processing Activities** with confirmation of how these conditions are met. Please click here to see the detailed additional conditions [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data].

The college also reserves the right to use other legal basis in its operational day to day activities where processing is necessary for **legitimate interests, performance of a contract, compliance with legal obligations, or in order to protect the vital interests of individuals**

If the College changes how it uses Personal Data, the College will need 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

The College endeavours to be as transparent about the processing of individual data as it can be and demonstrates this with the Privacy Notices available to students in their enrolment, staff in their induction process, parents of children under 16 and suppliers. Our **Privacy Notices** provide individuals with a summary of:

- the **purpose** for collecting the information
- the safeguards we put in place to **protect** your data and the college environment
- your **rights** in relation to the data we collect
- how long we **retain** your data for, and
- any third parties we **share** the information with.

Although we make reference to the generic **Retention** of the information in our privacy notices, we have many sources of data and many sets of information that we hold so it is difficult to detail all of them in the notice specifically whilst trying to keep it accessible and retain simplicity. The College **Record of Processing Activities** details all of the retention and destruction periods as set out by the individual processing laws or by the senior managers that control the use of that data. If you would like specific information on retention and destruction periods, please email acottrell@bsix.ac.uk

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.

If the College changes how it uses Personal Data then these privacy notices may be updated as required, but all individuals will be informed of any changes.

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

How we use your personal information in the college

We will use your information to manage your education, provide welfare and pastoral care, to track your progress so we can help you achieve the best you can.

This may include every day activities such as creating class lists for your teacher at the start of the course, providing registers for your tutor to mark your attendance, registering with the awarding bodies to allow us to enter you for your exams, or providing you with a support plan or exam assessment. For learners enrolling with the College for post 14 qualifications, the Learning Records Service will give us a learners' Unique Learner Number (ULN) and may also give us details about previous learning or qualifications. We also use this information to improve and develop teaching and services in the future.

The College will only share personal data with third parties as part of the statutory duties placed on us or as declared in the Privacy Notice. We do not share information about our learners with anyone without consent unless the law and our policies allow us to do so.

As part of the public task placed on us by the Education and Skills Funding Agency (ESFA) to fund education we have a duty to provide them with eligibility, enrolment and achievement data for all our learners.

We also share data concerning our 14-16 year-olds with the Department for Education (DfE) on a similar statutory basis. This data sharing underpins school funding, educational attainment policy and monitoring. To find out more about the data collection requirements placed on us by the Department for Education via the school census go to https://www.gov.uk/education/data-collection-and-censuses-for-schools, for more information on the data collected in the National Pupil Database go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information, for the DfE data sharing policy visit https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

We may also share the personal information that you give us with local authorities and schools but only in relation to your education, to provide appropriate support for you whilst you are with us, or to transfer information to other educational institutions you move to.

Young people have to remain in training or education until they are 18, so if you withdraw from our education programme before this age then we notify the local authority to highlight you may have become 'Not in Education, Employment or Training' (NEET). As part of the same legal duty we may also provide destinations data to them. In both circumstances this will only be shared with the relevant local authorities on a need to know basis.

We may also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year-olds under section 507B of the Education Act 1996. However, the parent / guardian of a 14-16 learner can request that only their child's name, address and date of birth is passed to their local authority or provider for the purposes of providing youth support services (once confirmed in writing to the 14-16 office). This right is transferred to the learner once he/she reaches age 16.

8. PERSONAL DATA MUST BE ACCURATE, KEPT UP TO DATE AND RELEVANT

The college has actively been taking steps to minimise the amount of information it collects and will continue to challenge internal processes to ensure data minimisation is at the forefront of our privacy by design development.

Enrolment forms and Learning Agreements for learners have been updated for the 18/19 academic year to ensure that we remove any personal information we do not need and that learners can opt out of providing information that is not mandatory.

New processes and systems are currently being developed for the 18/19 academic year to ensure personal data can be kept up to date by individuals themselves and accuracy remains paramount. Internal audits take place to review the accuracy of the data we keep, and any corrections are made.

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 who 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.

8.3. All College Personnel who 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 who access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.5. The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The College has a Data Rights Procedure which sets 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 this document.

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

This Data Protection Policy should be read in conjunction with the **Data Retention and Destruction Procedure** which details all of the college requirements and reasoning for why we retain information and how we delete or destroy the information we collect. This is linked to the College **Record of Processing Activities** where the retention periods for all information is detailed specifically in relation to the purpose that piece of information was collected for, any legal all public task requirements, and the operational activity undertaken.

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 Destruction 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 Destruction Procedure, 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

The College has put a **Data Breach Procedure** in place to both mitigate the risk of a breach occurring and to ensure there are appropriate procedures in place to respond. The objective of this policy is to enable staff to act promptly to contain any breaches that occur, minimising the risk associated with the breach and to take action if necessary to secure personal data and prevent further breaches.

The college expects its staff to embed security and prevention practices in their normal working day to ensure personal, or special category, data is protected for the purposes of college business and must take appropriate steps to safeguard this information. The College undertakes GDPR training for all staff to ensure college personnel are fully aware of the changes in the law, and fully understand their role duties and responsibilities in protecting and safeguarding the personal data we collect. This is a key part of the colleges security arrangements to help prevent a breach from occurring in the first place.

Additional IT security measures are also being implemented to protect the college networks and emails. If you discover a data breach, you must report this to our Data Protection Officer (DPO) immediately.

The Data Protection Officer is Adrian Cottrell and any breach, or suspected breach, can be sent for his attention on acottrell@bsix.ac.uk

All breaches big or small, regardless of the harm or potential harm, should be identified and reported. All College employees have a duty to report any breach they become aware of. Failure to follow the correct procedure or ignoring a possible data breach may result in disciplinary action.

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 College Personnel must comply with the College's Data Breach Procedure.

A 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

The College appoints contractors to work on our behalf to deliver aspects of college business that either the college is not best placed to deliver or is not suitably equipped to deliver. It may also utilise contractors for short term work, or where better economies of scale, breadth or expertise can be offered by a third party.

12.1. If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

12.2. One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

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

12.4. A Processor is considered as having been appointed where the College engages someone to perform a service on our behalf and as part of it they may get access to our Personal Data. Where we appoint a Processor in this way the College, as Controller, remain responsible for what happens to the Personal Data.

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

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

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

12.5.3. to ensure staff are subject to confidentiality obligations;

12.5.4. to take appropriate security measures;

12.5.5. to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

12.5.6. to keep the Personal Data secure and assist the Controller to do so;

12.5.7. to assist with the notification of Data Breaches and Data Protection Impact Assessments;

12.5.8. to assist with subject access/individuals rights;

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

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

12.5.11. to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

12.6. In addition, the contract should set out:

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

12.6.2. the nature and purpose of the processing;

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

12.6.4. the obligations and rights of the Controller.

13. INDIVIDUALS' RIGHTS

The new GDPR legislation clearly details that individuals have the right to be informed about how we collect and process their personal information, but it goes deeper than that in giving them more control about how their data is collected, stored, and what is done with it once the processing is complete. The College is fully aware of its legal obligations to allow individuals to exercise their rights over their Personal Data, and has therefore developed a specific **Data Rights Procedure** to ensure that all individuals understand the process for applying their rights.

Whilst the majority of information we request is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

14. MARKETING AND CONSENT

Marketing consists of any advertising or marketing communication that is directed to particular individuals. The College uses a variety of marketing techniques to attract learners, employers and the public.

The College can contact Individuals to send them marketing or to promote the College, but where this is done it will only be done in a legally GDPR compliant manner where we have obtained consent.

The College provides more detail in their privacy notices, learning agreements and college signage to state where profiling takes place; and will require an individual's consent as a "clear affirmative action" to be contacted for marketing purposes

The College is also 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 also applies to any electronic communication the college sends out including telephone calls, emails and text messages.

14.1. All electronic marketing communications from the College will ask individuals to opt in to the services they receive.

14.2. Alternatively, the College is able to market using a "soft opt in" if the following conditions are met:

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

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

14.2.3. 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.

15. AUTOMATED DECISION MAKING AND PROFILING

The College is carefully monitoring all of its operational activities where profiling or automated decision making occurs. There are some operational activities in the college where profiling occurs but any outcome or decision as a result of the profiling activity is ultimately made by human involvement. Automated decision making is very limited around the college, and nearly all processes have some human involvement at some point to ensure no individual is disadvantaged or treated unfairly.

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)

The College actively promotes a Privacy by Design approach and ensures Data Protection Impact. Assessments are undertaken when there is a change to a system, service or process.

The College has an IT Steering Group that oversees any new IT projects, software or system implementation at the college. Part of the rigorous process for approving new IT projects now includes GDPR compliancy checks for any new supplier. This will include assessing whether the supplier has appropriate IT infrastructure and security measures in place, as well as assessing their GDPR compliance in relation to Policies and Procedures should a data breach occur. If the Supplier is appointed part of this process will also include setting up data sharing agreements, and assessing whether a DPIA is required before the project implementation starts.

If the DPIA is required for an IT Project or an internal process change then the GDPR legislation requires the college to put in place a number of steps to control any such changes to processing.

16.1. Carry out a risk assessment in relation to the use of Personal Data for a new service, product, process or project. 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 period of the project. 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.

16.3. All DPIAs must be reviewed and approved by the Data Protection Officer. Any privacy risks identified should either be mitigated for with an appropriate solution or be monitored during the project and the DPIA revisited.

17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

The college does not consider that it transfers personal data outside the EEA, or any country where appropriate adequacy measures are not in place. This applies to our own personal data storage, or any company we use that are based overseas or their storage facilities are based overseas.

The college ensures it continually reviews its own processes and the compliance of its partners or contractors to ensure that we would be aware if any data transfers outside the EEA were required.

17.1. There are strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. The College must consider this when appointing a supplier outside the EEA, or a supplier with group companies outside the EEA, which may give access to the Personal Data to staff outside the EEA.

17.2. College Personnel must not export Personal Data, inside or outside the EEA, without the approval by the Data Protection Officer.