TABLE OF CONTENTS

If you require this document in an alternative format, please contact Hequality@tameside.ac.uk

1. INTRODUCTION AND SCOPE

1.1 Tameside College is committed to ensuring that all Personal Data collected is processed in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other related legislation. 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.

1.2 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 how the College handles uses, transfers and stores Personal Data.

1.3 The College has implemented this Data Protection Policy, alongside associated documentation, 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.

1.4 This policy applies to staff, students and all key stakeholders at Tameside College including governors, volunteers, parents/carers, visitors, contractors, and other community users. Compliance with the Act is the responsibility of all members of Tameside College. Any deliberate breach of the data protection policy may lead to disciplinary action.

1.5 It applies to all Personal Data stored electronically, in paper form, or otherwise.

1.6 College staff will be signposted to a copy of this Policy when they start and may receive notifications of revisions. This Policy does not form part of any member of the College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of College Personnel are obliged to comply with this Policy at all times. Any failure to follow the policy can therefore result in disciplinary proceedings.

1.7 Tameside College is registered as a Data Controller with the Information Commissioners Office (ICO) under Registration Number Z7345553.

1.8 If you have any queries concerning this Policy, please contact our Data Protection Officer at dpo@tameside.ac.uk who is responsible for ensuring the College's compliance with this Policy.

2. DEFINITIONS

2.1 College Personnel – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

2.2 Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it. A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

2.3 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.

2.4 Data Protection Officer – Our Data Protection Officer is Nils Elgar and can be contacted at: 0161 909-5709 (c/o Selina Moseley) or dpo@tameside.ac.uk. The DPO may delegate responsibility to a member of the Senior Management Team or other College Managers where appropriate.

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

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

2.7 Individuals – Living individuals who can be identified, directly or indirectly, from information that the College has. For example, an individual could be identified directly by name, or indirectly by

gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

2.8 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. any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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.

2.9 Processing - In relation to Personal Data, processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

2.10 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.

2.11 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. Please note that processing criminal offence data is also subject to additional controls.

3. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

3.1 All College Personnel must comply with this Policy, as well as associated data protection policies and documentation, and including the College's IT policies in relation to security as outlined in Section 17 **RELATED POLICIES**.

3.2 College Personnel must:

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

3.2.2 not release or disclose any Personal Data:

- outside the College; or
- inside the College to College Personnel not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

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

3.2.4 ensure they discuss any proposed new uses of Personal Data with the Data Protection Officer (DPO).

3.2.5 ensure that Personal Data is destroyed in accordance with the College's Data Retention Policy.

3.2.6 are responsible for undertaking data protection and information handling training as directed.

3.2.7 ensure that all information they provide to the College in relation to their employment is accurate and up to date. They must inform the College of any changes to the information they have provided.

4. DATA PROTECTION OFFICER'S RESPONSIBILITIES

4.1 The Data Protection Officer (DPO) is responsible for:

4.1.1 Advising on the implementation of this and related policies.

4.1.2 Keeping information law policies and procedures under review and developing policies and guidance as required.

4.1.3 Monitoring compliance with this and related policies, ensuring College data processing complies with data protection law.

4.1.4 Providing advice and guidance on data protection and wider information law matters.

4.1.5 Investigating Personal Data breaches and notifying the ICO and data subjects as necessary.

4.1.6 Responding to data subject rights requests (as well as requests under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004) within statutory time frames and maintaining compliance logs.

4.1.7 Maintaining the College's registration with the ICO and acting as point of contact with the ICO as necessary.

4.1.8 Raising data protection awareness and ensuring data protection training requirements are complied with.

5. TRAINING

5.1 The College will provide training to all individuals about their data protection responsibilities as part of the induction process.

5.2 Individuals whose roles require regular access to Personal Data will have a mandatory requirement to complete data protection training.

5.3 Staff are required to refresh their knowledge and understanding and will undertake mandatory training on a regular basis.

6. 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:

6.1.1 processed lawfully, fairly and in a transparent manner. The College maintains up to date Privacy Notices to ensure individuals are fully informed about what Personal Data is being processed and why. Where Personal Data is received 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 as soon as reasonably possible and in any event within one month.

The College identifies an appropriate lawful basis for processing as well as additional conditions to justify the processing of special category data and criminal offence data. As part of this the College maintains and publishes an Appropriate Policy Document

6.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The College ensures individuals are fully informed of the purpose of processing and records those purposes in privacy notices as well as wider documentation for accountability purposes. Should the purpose for which data is processed change over time or a new purpose arise, the College will only proceed if the new purpose is compatible with the original purpose, the individual consents to the new purpose or a clear legal provision requires or allows the new processing in the public interest.

6.1.3 adequate, relevant and limited to what is necessary for the purposes for which it is being processed. The College ensures it only collects data that is actually needed for its specified purposes. We periodically review data and delete any data that is not needed to fulfil those purposes.

6.1.4 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. The College ensures that data is recorded accurately and also records the source of the data provided. The College takes reasonable steps, having regard to the circumstances, the nature of the Personal Data and the purpose of processing, to ensure the accuracy of information.

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 legislation. The College has processes in place to respond to data subject rights requests appropriately and within statutory timescales.

6.1.5 kept for no longer than is necessary for the purposes for which it is being processed. The College maintains a Data Retention Policy Schedule that sets out how long all data, including special category data, shall be retained for. This Schedule is kept under regular review. The College also reviews the data it holds at appropriate intervals as part of its regular review of the Record of Processing Activity held. When data held is no longer needed for the purpose it was collected for, the College ensures it is deleted or anonymised.

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, they should contact the Data Protection Officer for guidance.

6.1.6 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. The College has implemented appropriate technical measures to ensure the security of data processed. The College keeps its Information Security Policy, as well as other policies such as Network Access Control Policy, Remote Access Policy, Password Policy, Anti-Virus Policy, Backup Policy, Business Continuity and Disaster Recovery Plans under regular review. The College ensures all staff undertake data protection training with annual refresher training.

6.2 In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them as part of its accountability obligations. 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. As part of this, we have published an Appropriate Policy Document in relation to our processing of Special

Category and Criminal Offence Data, we keep our Record of Processing Activity under regular review. The College also ensures that Data Protection Impact Assessments are carried out for processing likely to result in a high risk to individuals' interests.

6. LAWFUL USE OF PERSONAL DATA

6.1 Processing Personal Data will not be lawful without a valid lawful basis. Documenting our processing activities and the lawful basis on which the processing is justified is also a key part of our accountability obligation under the legislation.

6.2 To ensure that our processing of Personal Data is lawful, the College has carefully assessed how it uses Personal Data and has identified one of the six grounds set out in Article 6 of the UK GDPR as a valid basis on which to process the data before the processing begins. Further information on the lawful bases can be found here.

6.3 Where the College processes Special Category or Criminal Offence data, it has to show that one of a number of additional conditions is met. These are set out in Article 9 of the UK GDPR. These additional conditions have also been assessed and the College has identified which are applicable in order to justify its processing of special category or criminal offence data. Further information on the additional conditions for processing Special Category data can be found here.

6.4 Determining the correct legal basis for processing data can be difficult and more than one ground may be applicable. Please contact the Data Protection Officer on DPO@tameside.ac.uk for advice and guidance.

6.5 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. DATA SECURITY

7.1 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. Please see the following documents for further detail on this:

- IT Acceptable Use Policy
- Network Access Control Policy
- Remote Access Policy
- Password Policy
- Anti-Virus Policy
- Backup Policy
- Business Continuity Management Policy.

8. DATA BREACH

8.1 Whilst the College takes information security very seriously, unfortunately 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. In such an event College Personnel must comply with the College's Personal Data Breach Notification Policy. This sets out important obligations in the event of a Personal Data breach and so all College Personnel must ensure they are familiar with it to enable them to spot a breach or a near miss and to know what to do should such an event occur.

8.2 A Personal Data breach is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.' 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. Unauthorised use, processing or disclosure of Personal Data contrary to College Data Protection Policy is likely to be considered gross misconduct and dealt with under the College's Disciplinary Procedure.

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

- Confidentiality breach - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;
- Availability breach - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

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

8.4 The College ensures that all College Personnel who have access to Personal Data are appropriately trained in data protection according to their role in order to reduce the likelihood of Personal Data misuse. This also ensures that College Personnel are able to quickly recognise if a Personal Data breach has occurred to that swift action can be taken to mitigate the risks to data subjects and ensure compliance with the College's obligations in relation to data breaches.

9. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA

9.1 Under Data Protection legislation, the College may only appoint a contractor to process Personal Data on behalf of the College where the College has carried out sufficient due diligence and only where there are appropriate written contracts in place.

9.2 A Data Controller is considered as having appointed a Data Processor where it engages a third party to perform a service on its behalf, as part of which they will require or obtain access to that Controller's Personal Data. Where the College appoints a Data Processor in this way, it is the College which remains responsible for what happens to its Personal Data.

9.3 The legislation requires that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals which means that data protection due diligence must be undertaken on both new and existing suppliers. Once a Processor is appointed they must be audited periodically to ensure that they continue to meet contractual requirements in relation to Data Protection.

9.4 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 College Personnel 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 requests;
- 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.

9.5 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.

9.6 Any questions in relation to the College's use of Data Processors should be directed at the DPO at dpo@tameside.ac.uk.

10. INDIVIDUAL RIGHTS

10.1 Data protection law gives individuals greater control over their Personal Data through several rights which the College strives to facilitate effectively.

10.1.1 Requests can be made verbally or in writing to dpo@tameside.ac.uk. If a member of College Personnel receives a data subject rights request you should forward it to the DPO immediately and no later than within 24 hours of receipt. If the request is made verbally, please obtain as much information as possible about the request, including contact details for the data subject, and pass them immediately to the DPO. College Personnel must not make any attempt to deal with, or respond to, the request without authorisation from the Data Protection Officer.

10.1.2 The College must respond to data subject requests within one calendar month. It is possible to extend the time to respond by a further two months if the request is complex or if we have received a number of requests from the individual. The College will let the

individual know that the time limit needs to be extended within one month of receiving the request and will explain the reasons for the extension.

10.1.3 Generally, there is no fee for making a data subject rights request, however the College may charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive. Where the College charges a fee, we will contact the individual promptly to inform them. Please note that the College does not have to comply with the request until we have received the fee.

10.1.4 Some rights only apply in certain circumstances, depending on the lawful basis for processing. The College may refuse to comply with a request if an exemption applies or if a request is manifestly unfounded or excessive. Every request will be dealt with on a case by case basis. Further information on all data subject rights can be found at A guide to individual rights | ICO.

10.1.5 The Rights of Individuals Procedure will be followed by the College in responding to any data subject rights request.

10.1.6 If an individual has a complaint about the way in which their data subject rights request has been dealt with they should contact the Data Protection Officer at dpo@tameside.ac.uk.

10.1.7 If an individual remains dissatisfied, they have the right to complain to the Information Commissioner's Office www.ico.org.uk.

10.1.8 Please contact the Data Protection Officer at dpo@tameside.ac.uk if you wish to withdraw consent to processing.

10.2 The right to be informed

10.2.1 Individuals have the right to be informed about the collection and use of their Personal Data. This is a key transparency requirement under GDPR. The College must provide individuals with information including; the purpose for processing their Personal Data, the retention period for that Personal Data, and who it will be shared with. This is called privacy information.

10.3 The right of access

10.3.1 Individuals have the right to access the personal information that the College holds about them, by making a request, known as a 'subject access request'. An individual may appoint another person to act on their behalf in making a subject access request (SAR). When this happens, the College will need written evidence that the individual concerned has authorised a third party to make the application and may also require further identification for the person making the request so that the College can be confident of their identity.

10.3.2 If an individual makes a subject access request, the Data Protection Officer will tell him/her:

- Whether or not their data is processed and if so, why, the categories of Personal Data concerned and the source of the data if it is not collected from the individual.
- To whom their data is or may be disclosed, including to recipients located outside the European Economic Area and the safeguards that apply to such transfers.
- For how long their Personal Data is stored.
- Their rights to rectification or erasure of data, or to restrict or object to processing.
- Their right to complain to the Information Commissioner if they think the College has failed to comply with their data protection rights, and
- Whether or not the College carried out automated decision-making and the logic involved in any such decision-making.

- The College will also provide the individual with a copy of the Personal Data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

10.4 The right to rectification

10.4.1 Individuals have the right to have inaccurate Personal Data rectified or, depending on the purposes for processing, to have incomplete data completed. On receiving a request for rectification, the College will take reasonable steps to determine the accuracy of the data held and will restrict processing the Personal Data in question while we do this. Further information can be found here Right to rectification | ICO.

10.5 The right to erasure

10.5.1 The right to erasure is also known as the 'right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of Personal Data where there is no compelling reason for its continued processing. This applies only to data the College holds at the time the request is made, and not to data that may be created in the future. The right is not absolute and only applies in certain circumstances. Further information can be found here Right to erasure | ICO.

10.6 The right to restrict processing

10.6.1 As an alternative to the right to erasure, an individual can request that the way an organisation uses their Personal Data is limited. When processing is restricted, the College is permitted to store the Personal Data, but not to use it. The College is allowed to retain just enough information about the individual to ensure that the restriction is respected in future. This is not an absolute right and applies in certain circumstances. Further information can be found here Right to restrict processing | ICO.

10.7 The right to data portability

10.7.1 Individuals have the right to request Personal Data they have provided to a controller in a structured, commonly used and machine-readable format. This right isn't the same as subject access and is intended to give individuals a subset of their data. Individuals can receive their data and store it for future re-use or can request that a Controller transmits this data directly to another Controller. The right to data portability only applies in certain circumstances. Further information can be found here Right to data portability | ICO.

10.8 The right to object

10.8.1 Individuals have the right to object to the College processing their Personal Data in certain circumstances. The right to object to processing of Personal Data for the purposes of direct marketing is an absolute right. Therefore, when the College receives such a request it will suppress the Personal Data of the individual concerned retaining just enough to ensure that they do not receive direct marketing in future. Further information on the right to object can be found here Right to object | ICO.

10.9 Rights related to automated decision making including profiling

10.9.1 The College will not use Personal Data for the purposes of automated decision making that has legal or significantly similar effects on the individual unless the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by UK law; or
- based on the individual's explicit consent.

10.9.2 Where an organisation does use Personal Data in this way, individuals have the right to challenge such decisions, request human intervention in the process, express their own point of view and obtain an explanation from the College.

10.9.3 Where an organisation does use automated decision making, including profiling, it must:

- provide meaningful information about the way the decision-making process works, as well as explaining the significance and the envisaged consequences for the individual;
- use appropriate mathematical or statistical procedures;
- ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it;
- put appropriate technical and organisational measures in place, to minimise the risk of errors and so that inaccuracies can be corrected; and,
- secure Personal Data in a way that prevents discriminatory effects and is proportionate to the risks to the individual's rights.

11. MARKETING AND CONSENT

11.1 You will only be sent direct marketing from the College where you have given explicit consent to receive such communications from us. Where the College carries out any such marketing, it ensures that it does so in a manner compliant with both Data Protection legislation as well as with the Privacy and Electronic Communications Regulations (PECR).

11.2 You have the right to withdraw your consent at any time. To do so please contact the Data Protection Officer at dpo@tameside.ac.uk.

11.3 Alternatively, the College may be able to market using a "soft opt in" if the following conditions are met:

- contact details have been obtained in the course of a sale (or negotiations for a sale);
- the College are marketing its own similar services; and,

- the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

12. AUTOMATED DECISION MAKING AND PROFILING

12.1 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,

Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

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

12.3 College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer in order to ensure that the college is compliant with data protection legislation.

13. DATA PROTECTION BY DESIGN AND DEFAULT AND DPIAs

13.1 The concept of data protection by design seeks to ensure consideration of data protection issues at the outset and through the lifecycle of all processing activities. Data protection by default requires organisations to ensure that they only process the data that is necessary to achieve the specific purpose in hand. It links to the fundamental data protection principles of data minimisation and purpose limitation.

13.2 **Data Protection Impact Assessments (DPIAs)**

13.2.1 DPIAs are a fundamental part of the concept of data protection by design in assessing the technical and organisational measures needed to ensure that processing complies with the data protection principles. DPIAs are also a key part of the accountability obligations under the GDPR.

13.2.2 As such, a DPIA should be started as early as practical in the design of processing operations so that 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.

13.2.3 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
- consider the measures to address the risks identified.

13.2.4 All DPIAs must be reviewed and approved by the Data Protection Officer. Where a DPIA reveals a high risk which cannot be appropriately mitigated, the ICO must be consulted.

13.2.5 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. Alongside this trigger, there are certain specific circumstances in which a DPIA is mandatory, namely the following:

Under the GDPR a DPIA must be completed if you plan to:

- Use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

13.2.6 The ICO also requires completion of a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect Personal Data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

13.2.7 It is important to note that consideration of data protection issues and risks is not just for new projects but may need to be addressed in relation to existing processing if the risks are sufficiently high and/or the way an activity is being carried out has changed. If you are unsure whether a DPIA is needed or have any questions about the process, please contact the DPO at dpo@tameside.ac.uk.

13.2.8 The College uses the ICO's DPIA template which is available here.

14. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

14.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be considered whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to College Personnel outside the EEA.

14.2 In order to ensure that the College is compliant with Data Protection legislation College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

15. LOCATION AND ACCESS TO THE POLICY

The Data Protection Policy is available on the College website. Related policies and other documents are available via CollegeiP on the College network for staff and through course handbooks/inductions and the Student Portal for students.

16. RELATED POLICIES

- Anti-Virus Policy
- Appropriate Policy Document
- Backup Policy
- Data Retention Policy and Schedules
- IT Acceptable Use Policy
- Network Access Control Policy
- Password Policy
- Personal Data Breach Notification Policy
- Privacy Notices
- Remote Access Policy
- Business Continuity Management Policy

17. POLICY STATUS

Responsibility:	DPO, Nils Elgar (Clerk to the Corporation)
Approved by:	Senior Leadership Team
Review Date:	June 2024
Next Review Date:	June 2025

Review/Change History:

Version	Description/Detail of Update & Name of Person who has carried out Update	Approval	Date of Issue
2	Section 1: Inclusion of Governors as group on which College collects Personal Data.	SLT	June 2024

	Section 3.4: Updated contact details of DPO. N.B. Use of Selina's phone number. Section 6.1: Provide link to ICO for the legal grounds on which College collects personal information (rather than referencing College's Data Retention Policy). Section 6.2: Provide link to ICO for the conditions on which the College collects Special Categories of Personal Data (rather than referencing the College's Data Retention Policy. Section 7.1: Addition of Privacy Policy for Governors (still to be drafted) Sections 9.2 and 9.3: 'Data Retention Policy' (not 'Data Use and Retention Schedule').		