Hartlepool College of Further Education

Quality Assurance Policies & Procedures

DATA PROTECTION

Overview

Data protection legislation is complex and verbose; nevertheless this policy is critical to the operation of the College. This document is intended as a reference and, as such, a contents list is provided to enable users to quickly locate areas of specific interest in College operations.

Contents

1 POLICY STATEMENT

Hartlepool College of Further Education needs to collect personal information to effectively carry out our everyday business functions and activities to provide programmes and services to learners and clients. Such data is collected from learners, employees, suppliers and clients and may include (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, bank/credit card details, private and confidential information and sensitive information.

In addition, the College may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations. The College is committed to processing all personal information in accordance with the UK General Data Protection Regulation (UK-GDPR), UK data protection laws and any other relevant data protection laws and codes of conduct (collectively referred to as “the data protection laws”).

The College has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities. The College operates a 'Privacy by Design' approach, assessing

changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2 PURPOSE

The purpose of this policy is to ensure that the College meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the College has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

3 SCOPE

This policy applies to all staff within the College *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the College).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.1 DEFINITIONS

- ***"Biometric data"*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- ***"Binding Corporate Rules"*** means personal data protection policies which are adhered to by the College for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
- ***"Consent"*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***"Cross Border Processing"*** means processing of personal data which:
    - takes place in more than one State; or
    - which substantially affects or is likely to affect data subjects in more than one State
- ***"Data controller"*** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by UK law, the controller or the specific criteria for its nomination may be provided for by UK law.
- ***"Data processor"*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***"Data protection laws"*** means for the purposes of this document, the collective description of the UK-GDPR, Data Protection Act (2018) and any other relevant data protection laws that the College complies with.

- ***"Data subject"*** means a living individual (natural person) who is the subject of personal data
- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"Genetic data"*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- ***"Personal data"*** means 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.
- ***"Processing"*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- ***"Profiling"*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with European Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***"Supervisory Authority"*** means an independent public authority which is established by the UK Government.
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the data subject, under the College's direct authority
- ***"UK-GDPR"*** *means the UK's implementation of the General Data Protection Regulation (GDPR).*

4 DATA PROTECTION BACKGROUND

The UK initially put in place The Data Protection Act 1984 to regulate the use of processed information that related to individuals. However, in 1995 the introduction of EU Directive 95/46/EC which set aims and requirements for member states on the protection of personal data when processing or sharing, meant an updated Act was required.

The UK subsequently developed and enacted The Data Protection Act 1998 (DPA) to ensure that British law complied with the EU Directive and to provide those with obligations under the Act, with updated rules, requirements and guidelines for processing and sharing personal data.

2018 marks the 20th anniversary of the DPA enactment and whilst there have been periodical additions or alterations to the Act, technology has advanced at a far faster rate, necessitating new regulations for the current digital age. The past 20 years has also seen a vast increase in the number of businesses and services operating across borders, further highlighting the international inconsistency in international data protection laws.

For this reason, in January 2012, the European Commission proposed a new regulation applying to all EU Member States and bringing a standardised and consistent approach to the processing and sharing of personal information across the EU.

4.1 NATIONAL DATA PROTECTION LAW

As the College is in the UK, it is obligated under the UK-GDPR and the UK's Data Protection Act (2018) that implements the GDPR into UK law. Our data protection policies and procedures adhere to both the UK-GDPR and Data Protection Act requirements, as applicable to our business type.

4.2 GENERAL DATA PROTECTION REGULATION (GDPR)

The *General Data Protection Regulation (GDPR (EU)2016/679)* was approved by the European Commission in April 2016 and applies to all EU Member States with effect from 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States. The UK incorporated GDPR into the UK Data Protection Act (2018) and even though the UK has left the EU, the provisions of GDPR still apply in the UK. The UK's implementation of the General Data Protection Regulation is known as UK-GDPR and is almost synonymous except for some deviations regarding waivers of data protection compliance for some national security and immigration issues.

As the College processes personal information regarding individuals (*data subjects*), it is obligated under the UK-General Data Protection Regulation (UK-GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles. For the purposes of this QAP GDPR and UK-GDPR are interchangeable.

4.2.1 PERSONAL DATA

Information protected under the GDPR is known as *"personal data"* and is defined as:

"Any information relating to an identified or identifiable natural person; 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."

The College ensures that a high level of care is afforded to personal data falling within the GDPR's 'special categories' *(previously sensitive personal data*), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the *'Special categories of Personal Data'* the GDPR advises that:

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

4.2.2 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject *('lawfulness, fairness and transparency')*

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes *('purpose limitation')*

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed *('data minimisation')*

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay *('accuracy')*

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject *('storage limitation')*

f) 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 *('integrity and confidentiality')*.

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' ('accountability')* and requires that organisations show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

4.3 THE INFORMATION COMMISSIONERS OFFICE (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes:

- The Data Protection Act 2018
- UK-General Data Protection Regulation *(post-2019)*
- The Privacy and Electronic Communication Regulations 2019
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004

The ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.

The College is registered with ICO and appears on the Data Protection Register as a controller of personal information.

The College's Data Protection Registration Number is Z7250373.

4.4 DATA PROTECTION OFFICER

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on organisations to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by an organisation where:

- The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

The College has appointed a designated Data Protection Officer and has done so in accordance with the GDPR requirements and ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting the College in monitoring its internal compliance with the Regulation and supporting and advising employees and associated third parties with regards to the data protection laws and requirements.

5 OBJECTIVES

The College is committed to ensuring that all personal data processed by the College is completed in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. The College will ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The College has developed the objectives below to meet its data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The College will ensure that:

- It protects the rights of individuals with regards to the processing of personal information
- It will develop, implement and maintain a data protection policy, procedure, audit plan and training programme for compliance with the data protection laws
- Every business practice, function and process carried out by the College, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where the College has verified and met the lawfulness of processing requirements
- It only processes special category data in accordance with the GDPR requirements and in compliance with the Data Protection Act Schedule 1 conditions
- It records consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees are competent and knowledgeable about their GDPR obligations and are provided with relevant training in the data protection laws, principles, regulations and how they apply to their specific role
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- It will maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- It will monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- It will have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- It appoints a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- It will have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data the College processes is obtained, used, stored and shared. The audit program is reviewed against data protection policies, procedures and the relevant regulations to ensure continued compliance
- It will store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice
- Where applicable, the College maintain records of processing activities in accordance with the Article 30 requirements
- It has developed and documented appropriate technical and organisational measures and controls for

personal data security and has a robust Information Security programme in place

6 GOVERNANCE PROCEDURES

6.1 ACCOUNTABILITY & COMPLIANCE

Due to the nature, scope, context and purposes of processing undertaken by the College, frequent risk assessments and information audits will be carried out to identify, assess, measure and monitor the impact of such processing. The College has implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through its documentation and practices.

College governance objectives are to:

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that the College has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

6.1.1 PRIVACY BY DESIGN

The College operates a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via College processes, systems and activities. The College has developed controls and measures, detailed below, that help to enforce this ethos.

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of a minimalist approach. The College only ever obtains, retains, processes and shares data that is essential for carrying out our services and/or meeting our legal obligations and will only retain data for as long as is necessary.

College systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables the College to reduce data protection risks and breaches and supports its compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes:

- Electronic collection *(i.e. forms, the website, surveys etc.*) only have the fields that are relevant to the purpose of collection and subsequent processing. The College will not include *'optional'* fields, as optional denotes that it is not necessary to obtain

- Physical collection *(i.e. face-to-face, telephone etc*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- The College have SLA's and bespoke agreements in place with third-party controllers who send the College personal information (*either in our capacity as a controller or processor).* These state that only relevant and necessary data is to be provided as it relates to the processing activity the College is carrying out
- The College has documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement
- Forms, contact pages and any documents used to collect personal information are reviewed regularly to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing

Pseudonymisation

The College may utilise pseudonymisation where possible to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (*personal identifiers*). Encryption and partitioning may also be used to protect the personal identifiers, being kept separate from the pseudonymised data sets.

When using pseudonymisation, the College will ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation can mean that the data subject is still likely to be identified indirectly and, as such, the College will use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption

The College may utilise encryption as a further risk prevention measure for securing the personal data that the College holds. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

The College will utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction

Our *Privacy by Design* approach means that the College uses College-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the College's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose have access to personal information. Special category data is restricted at all levels and can only be accessed by staff with authorised permission to do so.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and

special category information which is only available in a paper format without pseudonymisation options (*e.g. copies of medical reports or funding claims information*). Where this is necessary, the College utilises a tiered approach to minimise the information the College holds and/or the length of time the College holds it for. Steps include:

- In the first instance, the College always ask the initial data controller to send copies of any personal information records directly to the data subject
- Where step 1 is not possible or feasible, the College will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (*i.e. when the data is being passed to a third-party for processing and not directly to the data subject*)
- When only mandatory information is visible on the hard copy data, the College will utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied
- Recipients (*i.e. the data subject, third-party processer*) are reverified and their identity and contact details checked
- The Data Protection Officer authorises the transfer and checks the file(s) attached and encryption method and key
- Once confirmation has been obtained that the recipient has received the personal information, where possible *(within the legal guidelines and rules of the data protection laws*), the College will destroy the hard copy data and delete the sent message
- If for any reason a copy of the paper data must be retained by the College, the College will use a physically safe store for such documents as opposed to our standard archiving system

6.1.2 INFORMATION AUDIT

To enable the College to fully prepare for and comply with the data protection laws, a College-wide data protection information audit will be conducted biennially to allow it to record, categorise and protect the personal data that the College holds and process.

The audit identifies, categorises and records all personal information obtained, processed and shared by our College in our capacity as a controller/processor and has been compiled on a central register which includes:

- What personal data the College holds
- Where it came from
- Who the College shares it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers

6.2 LEGAL BASIS FOR PROCESSING *(LAWFULNESS)*

At the core of all personal information processing activities undertaken by the College, is the assurance and verification that the College are complying with Article 6 of the GDPR and our lawfulness of processing

obligations. Prior to carrying out any personal data processing activity, the College will identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure the College is using the most appropriate legal basis.

The legal basis is to be documented on the information audit register, in our Privacy Notices and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. *Data is only obtained, processed or stored when the College has met the lawfulness of processing requirements where:*

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the College are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the College
- Processing is necessary for the purposes of the legitimate interests pursued by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).*

6.2.1 PROCESSING SPECIAL CATEGORY DATA

Special categories of Personal Data are defined in the data protection laws as:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the College processes any personal information classed as special category or information relating to criminal convictions, the College will do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Act's Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

The College will only ever process special category data where:

- The data subject has given explicit consent to the processing of the personal data
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim

- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Schedule 1, Parts 1, 2 & 3 of The Data Protection Act provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organisations are obligated to meet when processing such data.

Where the College processes personal information that falls into one of the above categories, the College will have adequate and appropriate provisions and measures in place prior to any processing. *Measures include:*

- Verifying our reliance on one of the data protection laws Article 9(1), and where applicable The Data Protection Act Sch.1, Pt.1, Pt.2 and/or Pt.3 conditions prior to processing
- Documenting the Schedule 1 condition and Article 6(1) legal basis relied upon from processing on our Processing Activities Register (*where applicable)*
- Having an appropriate policy document in place when the processing is carried out, specifying College:
    - procedures for securing compliance with the data protection laws principles
    - policies as regards the retention and erasure of personal data processed in reliance on the condition
    - retention periods and reason *(i.e. legal, statutory etc)*
    - procedures for reviewing and updating our policies in this area

6.2.2 RECORDS OF PROCESSING ACTIVITIES

As an organisation with 250 or more employees or where the following conditions apply:

1. Processing personal data could result in a risk to the rights and freedoms of individual
2. The processing is not occasional
3. The College process special categories of data or criminal convictions and offences
4. Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

The College maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the Supervisory Authority upon request.

Acting in the capacity as a controller *(or a representative*), our internal records of the processing activities carried out under our responsibility, contain the following information:

- Our full name and contact details and the name and contact details of the Data Protection Officer. Where applicable, the College will also record any joint controller and/or the controller's representative
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed *(including any recipients in third countries or international organisations)*
- Where applicable, transfers of personal data to a third country or an international organisation *(including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)*
- Where possible, the envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures as outlined in section 12 of this document *(pursuant to Article 32(1) of the data protection laws)*

Acting in the capacity as a processor (*or a representative*), our internal records of the categories of processing activities carried out on behalf of a controller, contain the following information:

- The full name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
- The categories of processing carried out on behalf of each controller
- Where applicable, transfers of personal data to a third country or an international organisation *(including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)*
- A general description of the processing security measures as outlined in section 13 of this document *(pursuant to Article 32(1) of the data protection laws)*

As part of our obligations under the UK's Data Protection Act, Sch.1, Pt.4, where the College is required to maintain a record of its processing activities in its capacity as a controller and is processing special category or criminal conviction data, as specified in Sch.1, Pt.1-3 of the Act, the College also records the following information on the register:

- Which condition is relied on?
- How the processing satisfies Article 6 of the data protection laws (*lawfulness of processing*)
- Whether the personal data is retained and erased in accordance with the policies described in paragraph 30(b) of the Data Protection Act (*and if not, the reasons for not following those policies*).

6.3 THIRD-PARTY PROCESSORS

The College may utilise external processors for certain processing activities. In such cases the College will use information audits to identify, categorise and record all personal data that is processed outside of the College, so that the information, processing activity, processor and legal basis are all recorded, reviewed and are easily

accessible. Such external processing includes (but is not limited to):

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Hosting or Email Servers
- Credit Reference Agencies
- Direct Marketing/Mailing Services

The College has strict due diligence procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. The College obtain appropriate documents, certifications, references and ensures that the processor is adequate, appropriate and effective for the task the College are employing them for.

The College audits their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always uppermost when choosing a processor and the College understands the importance of adequate and reliable outsourcing for processing activities as well as its continued obligations under the data protection laws for data processed and handled by a third-party.

The College will draft bespoke Service Level Agreements (SLAs) and contracts with each processor as per the services provided and have a dedicated Processor Agreement template that details:

- The processor's data protection obligations
- The College's expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without the College's prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The Processor Agreement and any associated contract reflects the fact that the processor:

- Processes the personal data only on the College's documented instructions
- Seeks the College's authorisation to transfer personal data to a third country or an international organisation (*unless required to do so by a law to which the processor is subject*)
- Shall inform the College of any such legal requirement to transfer data before processing

- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the College in ensuring compliance with its obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the College after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the College all information necessary to demonstrate compliance with the obligations set out in the agreement and contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the College immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

6.4 DATA RETENTION & DISPOSAL

The College has defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as the well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances.

7 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the College. The College therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, the College will utilise proportionate methods to map out and assess the impact ahead of time.

Where the College must or is considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, the College will always carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

Pursuant to Article 35(3) and Recitals 84, 89-96, the College considers processing that is likely to result in a high risk to include:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences

- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIAs enables the College to identify the most effective way to comply with its data protection obligations and ensure the highest level of data privacy when processing. It is part of the College's 'Privacy by Design' approach and allows it to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either:

- Eliminated
- Reduced
- Accepted

8 DATA SUBJECT RIGHTS PROCEDURES

8.1 CONSENT & THE RIGHT TO BE INFORMED

The collection of personal and sometimes special category data is a fundamental part of the programmes/services offered by the College and the College therefore has specific measures and controls in place to ensure that it complies with the conditions for consent under the data protection laws.

The data protection law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.*

Where processing is based on consent, the College has reviewed and revised all consent mechanisms to ensure that:

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand

- Pre-ticked, opt-in boxes are never used
- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), the College will ensure that the consent is separate from the other matters and is not a precondition of any service (*unless necessary for that service)*
- Along with the College name, the College will also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and the College will have controls in place to ensure that the College can demonstrate consent in every case
- The College will keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of the College name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- The College has ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including:
    - Opt-out links in mailings or electronic communications
    - Opt-out process explanation and steps on the website and in all written communications
    - Ability to opt-out verbally, in writing or by email
- Consent withdrawal requests are processed immediately and without detriment
- Where services are offered to children, age-verification and parental-consent measures have been developed and are in place to obtain consent where required by data protection law
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

8.1.1 CONSENT CONTROLS

The College maintains rigid records of data subject consent for processing personal data and will always be able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. The College will also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language.

Consent to obtain and process personal data is obtained by the College through methods including:

- Face-to-Face
- Telephone

- In Writing
- Email/SMS
- Electronic *(i.e. via a website form*)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilises a demonstrable opt-in mechanism. Where consent is obtained verbally, the College utilise scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and/or share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that the College is compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

8.1.2 CHILD'S CONSENT

While the GDPR states that a child's age is defined as under 16; the UK's Data Protection Act reduces this age to ***13 years***, as per Article 8(1) of the data protection laws what advises that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."*

The data protection laws state that where processing is based on consent and the personal data relates to a child who is below the age of 13 years**,** such processing is only carried out by the College where consent has been obtained by the holder of parental responsibility over the child.

The College will have mechanisms in place to verify the age of any child prior to obtaining consent and review such consents annually for transferring from parental consent over to the child after age 13.

8.1.3 ALTERNATIVES TO CONSENT

The College recognises that there are six lawful bases for processing and that consent is not always the most appropriate option. The College has reviewed all processing activities and will only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, the College will ensure that none of the below are factors:

- Where the College asks for consent but would still process it even if it was not given *(or withdrawn).* If the College would still process the data under an alternative lawful basis regardless of consent, the College recognises it is not the correct lawful basis to use
- Where the College asks for consent to process personal data as a precondition of a service the College is offering, it is not given as an option and consent is not appropriate
- Where there is an imbalance in the relationship, i.e. with employees

8.1.4 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), the College will provide the following information in all instances, in the form of a privacy notice:

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) *"processing is necessary for the purposes of the legitimate interests pursued by a third party",* details of the legitimate interests
- The recipients or categories of recipients of the personal data *(if applicable)*
- If applicable, the fact that the College intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where the College intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards the College has put into place the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as the well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as the well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as the well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

8.2 PRIVACY NOTICE

The College defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time the College collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*.

The Privacy Notice includes Article 13 (*where collected directly from individual*) or *14 (where not collected directly)* requirements and provides individuals with all the necessary and legal information about how, why and when the College processes their data, along with their rights and obligations.

There will be a link to the Privacy Notice on the College the website. This can be provided as a copy in physical and digital formats upon request. The notice is the user facing policy that provides the legal information on how the College will handle, process and disclose personal information.

The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection:

- Via the College website
- Linked to or written in the footer of emails
- Worded in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Verbally via telephone or face-to-face
- Via SMS
- Printed media, adverts and financial promotions
- Digital Products/Services
- On Mobile Apps
- Automated phone service

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, the College has tested, assessed and reviewed its privacy notice(s) to ensure usability, effectiveness and understanding.

The College will follow the ICO preferred steps for testing, reviewing and auditing its privacy notice(s) and opt-in consent formats prior to use and to record such assessments.

1. Privacy Notices are approved by the Data Protection Officer using the data protection laws requirements and with Supervisory Authority guidance
2. The College may utilise a select user base to test the Privacy Notice in its varying formats and provide a feedback form for completion
3. Final Privacy Notice(s) will be authorised by Senior Management before use

Where the College relies on consent to obtain and process personal information, the College will ensure that it is:

- The consent requirement id displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways the College will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing

- Includes a separate unticked opt-in box for direct marketing

8.3 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where the College obtains and/or processes personal data that has **not** been obtained directly from the data subject, the College ensures that the information disclosures contained in Article 14 are provided to the data subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

In addition to the information disclosures in section 8.1.4, where personal data has not been obtained directly from a data subject, the College also provides them with information about:

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure.

Where the College intends to further process any personal data for a purpose other than that for which it was originally obtained, the College will communicate this intention to the data subject prior to doing so and where applicable, process only with their consent.

Whilst the College follows best practice in the provision of the information noted in the relevant section of this policy, the College reserves the right not to provide the data subject with the information if:

- They already have it and the College can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by UK law to which the College is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by UK law, including a statutory obligation of secrecy

8.3.1 EMPLOYEE PERSONAL DATA

As per the data protection law guidelines, the College does not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how the College process their data and why.

All employees are provided with a Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information the College collects and processes about them.

8.4 THE RIGHT OF ACCESS

The College has ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information will be provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where the College does not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

8.4.1 SUBJECT ACCESS REQUEST

Where a data subject asks the College to confirm whether it holds and processes personal data concerning him or her and requests access to such data; the College will provide them with:

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the College from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the Data Protection Officer as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs should be completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, the College will provide the information in a commonly used electronic format, unless an alternative format is requested.

8.5 DATA PORTABILITY

The College will provide all personal information pertaining to a data subject to them on request and in a format, that is easy to disclose and read and will comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that the College comply with Article 20 of the data protection laws concerning data portability, the College will keep a commonly used and machine-readable format of personal information where the processing is based on:

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, the College will transmit the personal data directly from the College to a designated controller, where technically feasible.

The College may utilise the following formats for the machine-readable data:

- HTML
- CSV
- XML
- PDF
- XHTM

All requests for information to be provided to the data subject or a designated controller are completed free of charge and within 30 days of the request being received. If for any reason, the College does not act in responding to a request, the College will provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

8.6 RECTIFICATION & ERASURE

8.6.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by the College is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data

subject or controller informs us that the data the College holds is inaccurate, the College will take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The Data Protection Officer will be notified of the data subjects request to update personal data and is responsible for validating the information and arranging rectification of errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, the College will add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, the College will rectify the error within 30 days and inform any third party of the rectification if the College has disclosed the personal data in question to them. The data subject will be informed in writing of the correction and where applicable, will be provided with the details of any third-party to whom the data has been disclosed.

If for any reason, the College is unable to act in response to a request for rectification and/or completion, the College will always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.6.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, the College complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the College is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

8.7 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where the College restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subject's request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The College will apply restrictions to data processing in the following circumstances:

- Where an individual contests the accuracy of the personal data and the College are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and the College are considering whether the College have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure

- Where the College no longer needs the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and the College has disclosed such data to a third-party, the College will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. The College will also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, the College is unable to act in response to a request for restriction, the College will always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.8 OBJECTIONS AND AUTOMATED DECISION MAKING

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. The College provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. Individuals have the right to object to:

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where the College processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*. The College reserves the right to continue processing such personal data where:

- The College can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where the College is processing personal information for direct marketing purposes under a previously obtained consent, the College will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the College will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

The College has carried out a system audit to identify automated decision-making processes that do not involve human intervention. The College also assesses new systems and technologies for this same component prior to implementation. The College understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the data protection laws, the College aims to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an

individual and on our College website, the College advise individuals of their rights not to be subject to a decision when:

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, the College will use automated decision-making processes within the guidelines of the regulations. Such instances include:

- Where it is necessary for entering into or performance of a contract between the College and the individual
- Where it is authorised by law *(e.g. fraud or tax evasion prevention)*
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where the College uses automated decision-making processes the College will always inform the individual and advise them of their rights. The College will also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

9 OVERSIGHT PROCEDURES

9.1 SECURITY & BREACH MANAGEMENT

Alongside our *'Privacy by Design'* approach to protecting data, the College ensures the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our Information Security Policies provide the detailed measures and controls that the College take to protect personal information and to ensure its security from consent to disposal.

The College carries out information audits to ensures that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). The College has implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the College has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

10 TRANSFERS & DATA SHARING

The College takes proportionate and effective measures to protect personal data held and processed by us at all times, however the College recognises the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, the College utilises a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods.

The College will use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom the College deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

11 AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by the College to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, the College will also carry out regular audits and compliance monitoring processes with a view to ensuring that the measures and controls are in place to protect data subjects and their information and are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that the College is protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to CLC and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to:

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

12 TRAINING

Through its commitment and robust controls, the College will ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Arrangements for new and existing employees training, assessment and support will include:

- GDPR Workshops & Training Sessions

- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the data protection laws requirements and out own objectives and obligations around data protection.

13 PENALTIES

The College understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. The College respects the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where the College fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees will be made aware of the severity of such penalties and their proportionate nature in accordance with the breach. The College recognise that:

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to £8,700,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to £17,500,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

14 RESPONSIBILITIES

The College has appointed a Data Protection Officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the College, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with relevant managers to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.