SEG International College Data Protection Policy

1. General Policy Statement

1.1 SEG International College is committed to the protection of individuals' rights and privacy. The processing of personal data such as the collection, recording, use, and storage of personal information must be dealt with lawfully and correctly in accordance with this policy. All information containing personal data must be protected against unauthorised access, accidental loss or destruction, modification or disclosure.

1.2 The College regards the lawful and correct treatment of personal data as important to its successful operation, and to maintain confidence with our students and staff and other stakeholders.

2. Purpose and Scope

2.1 The College needs to process certain personal data in order to carry out its functions. These data relate to:

- Staff in relation to their contract of employment
- Prospective applicants and applicants to process applications and ensure they are properly informed of the study opportunities
- Students in relation to their studies
- Attendees to various events organised by the College
- Contractors
- Other third parties with whom it has dealings.

2.2 The College needs to collect, store, use, transfer and dispose of this data in order to fulfil its purposes as set out in the 1998 Education Reform Act to undertaken Further and Higher Education and Research and to exercise other powers granted under the Act. These include to undertake and administer students' education, to employ staff and undertake research. It also needs to meet its legal obligations to funding bodies, professional bodies, and the government.

2.3 This policy has been drawn up to ensure that all data is processed in accordance with the **General Data Protection Regulations** and the **Data Protection Act (2018)** which together form the Data Protection Legislation. This Policy sets out what the College is required to do to ensure correct and

lawful processing of personal data, to ensure that all staff, students and other workers who process personal data on behalf of the College are doing so in accordance with the Data Protection principles.

2.4 The Policy applies to all staff, students, governors, suppliers, contractors and others with whom the College has dealings.

3. Definition

Data Protection Legislation "Data Protection Legislation" refers to both the General Data Protection Regulations (2018) and the Data Protection Act (2018).

Personal Data "Personal Data" means 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'

Special Category Data "Special Category data" consists of personal data relating to:

- ethnic origin,
- physical and mental health (including, for example, details of the reasons for an individual's sick leave),
- sex life,
- genetics
- biometrics (where used for ID purposes)
- religion or belief,
- political opinion
- Trade Union membership.

Greater protections are required when processing this data. Criminal conviction data should be treated with similar care.

Processing "Processing" means obtaining, recording, holding or adding to the information or data or carrying out any operation or set of operations on the information or data.

Data Subject "Data subject" means an individual who is the subject of the personal data.

Data Controller "Data controller" means a person who or organisations which (either alone or jointly or in common with other persons/organisations) determines the purposes for which, and the manner in which, any personal data is processed. In this case, this means the College or nominated individuals acting on behalf of and with the authority of the College.

Data Processor "Data Processor" means any person (other than a member of staff) or organisation who processes data on behalf of the College.

Data Protection Impact Assessment "Data Protection Impact Assessment" means a formal assessment of the impact of processing on the individual including the risks and any impact on their rights and freedoms.

Breach A "breach" is any incident, or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data.

Data Protection Officer (DPO) ensures that the College applies the laws protecting individuals' personal data.

Staff Unless otherwise applicable, all references to staff include all current, past and prospective staff, full-time, part-time staff as well as agency workers, temporary workers and contractors.

Students Unless otherwise applicable, all references to students include all current, past and prospective students, whether full-time or part-time.

4. Data Protection

4.1 Data Protection is concerned with making sure that organisations handle personal data in a responsible way. It sets out legal obligations on how personal data is to be handled in relation to its collection, usage, storage, destruction, transfer and disclosure.

4.2 The Legislation applies to any information about a living individual (e.g. students, staff members, alumni and visitors etc.). Essentially, staff who handle any information about people as part of their job will need to comply with this Data Protection Policy.

5. Data Protection Principles

5.1 The GDPR sets out the main principles for organisations when processing data. In accordance with Article 5 of the GDPR, the College must ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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 not be considered to be incompatible with the initial purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 As well as being responsible for compliance, the College also has the obligation under Article 5(2) of the GDPR to be able to demonstrate compliance with the above principles.

6. Lawful basis for processing

6.1 The College must determine the lawful basis for processing before starting any collection of personal data. The lawful bases for processing are set out in Article 6 of the GDPR and at least one of these must apply whenever personal data is processed:

- Consent: the individual has given clear consent to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract with the individual, or because they have asked the College to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone’s life.

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

- Legitimate interests: the processing is necessary for the College's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply when the College is processing data to perform its official tasks).

6.2 In addition to having one of the lawful bases outlined above, the processing must also be necessary.

7. Special Category data

7.1 In order to process special categories data, the College must also ensure that one of the following from Article 10 of the GDPR applies as well as one of the legal bases outlined in paragraph 6 above:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- 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
- 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 relates to personal data which are manifestly made public by the data subject[1];
- 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, on the basis of EU or UK law[2] which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or UK law or pursuant to contract with a health professional;
- processing is necessary for reasons of public interest in the area of public health;

[1] As outlined in the GDPR is not relevant to the College
[2] As outlined in the Data Protection Act (2018)

- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7.2 The Data Protection Act (2018) sets out further clarification of these lawful bases. Where processing of special category data is being undertaken, the data owner must ensure that processing is in accordance with Schedule 1 of the Act. For example, it clarifies that the legal basis processing of special categories data for monitoring purposes is 'substantial public interest'.

8. Criminal Conviction data

8.1 The legislation also sets out the requirements for processing criminal convictions and the particular safeguards which need to be in place. Where the College is processing criminal convictions, it must ensure that it has identified a lawful basis under Section 8 as outlined and one from Section 9. The Data Protection Act clarifies these.

10.2 In addition to determining a lawful basis, the College must also document its procedures for processing criminal convictions in an appropriate policy. These are as follows:

- the processing criminal conviction data for all students on courses leading to a professional registration and the policy and procedure for assessing is subject to the Regulations for Disclosure and Barring Service Checks and the Fitness to Practise Regulations;
- the processing criminal conviction data for applicants and students who are not on courses leading to professional registration is subject to the Regulations for the consideration of applicants and students with a criminal conviction;
- the processing criminal conviction data for job candidates and staff is subject to the Staff Policy and Procedure for Criminal Convictions, Disclosures And Barring.

9. The rights of the individual

9.1 The College must respect individuals' rights when processing personal data. These are enshrined in the legislation as follows:

1. The right to be informed
2. The right of access

3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

9.2 The rights above depend upon the lawful basis for processing. For example, the right to erasure only applies where the lawful basis for processing is consent. Where public task, legitimate interests, contractual basis or a legal requirement are used as the basis for processing, the right of rectification, restriction and the right to object are also limited to ensuring that the data is accurate before it can be processed.

9.3 The right to be informed is, however, a key right and applies in all circumstances (see Transparency below).

10. Data protection by default

10.1 Where the College is undertaking new processing (e.g. it is collecting a new type of data or it is implementing a new system or process), it must consider building in data protection from the outset, including the organisational and technical measures to ensure appropriate security.

10.2 This may include undertaking a Data Protection Impact Assessment (DPIA) which is required for significant processing and where there are significant risks. Where a DPIA is not required, the College must still consider the risks to the individual of processing and how these risks will be mitigated and to document this assessment. This is undertaken by use of the Permission to Process Data Form available from IT. The DPO will advise on what is required.

10.3 New processing must be approved before collection is started and signed off by the DPO.

11. Data minimisation

11.1 Under GDPR, the College has an obligation to ensure that it collects only what data is necessary. Those who are collecting data should, therefore, ensure that it is limited to what is required.

11.2 Staff are required to assess whether any data being collected is necessary for the proposed purpose. Where processing can take place without this data it should not be collected

12. Transparency

12.1 The College needs to provide specific information to people about how it processes their personal data. This information needs to be actively provided to individuals in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

12.2 To provide this information, the College must provide a privacy notice. The College must ensure that the statement is targeted to the data subjects, particularly where children are being asked to provide data. It should be noted that the UK Government has been determined that the age at which children can consent to the use of their data is 13.

12.3 The Privacy Statement must include the following:

- The name and contact details of the College
- The contact details of the DPO
- The purposes of the processing
- The lawful basis for the processing
- The categories of personal data obtained
- The recipients or categories of recipients of the personal data
- The details of transfers of the personal data to any third countries or international organisations
- The retention periods for the personal data
- The rights available to individuals in respect of the processing
- The right to withdraw consent
- The right to lodge a complaint with a supervisory authority
- The source of the personal data
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data
- The details of the existence of automated decision-making, including profiling.

12.4 The Privacy Notices must be published on the College website and made available to the data subjects. Where processing is taking place that is not covered in an existing statement, a Privacy Notice for that processing must be published.

12.5 In addition to the privacy notices, the College is also required to inform data subjects of the purposes and use of data at the point of collection. Any College forms (whether paper-based or web-

based) that gather data on an individual should contain a summary of the Privacy Notice which explains the following:

- Why the data is being gathered and how the data will be used,
- To whom the data may be disclosed to within the College and to any outside third parties,
- Consent where this the legal basis of processing.

12.6 Staff may only process data for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Legislation. This means that personal data must not be collected for one purpose and then used for another purpose. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. The only exception to this is the use of research data.

13. Staff Responsibilities for data protection

13.1 The College as a corporate body is the data controller and staff have the responsibilities as set out below to deliver its commitment to the protection of rights and privacy of individuals (including students, staff and others) in the processing of personal data.

13.2 Heads of Departments are responsible for developing and maintaining good information handling practice within the College in accordance with this Policy and the Information Security Policy. They must maintain accurate records of the data processed in their department in accordance with the requirements of this policy. They must ensure that individuals are clear about what data they hold through an appropriate Privacy Notice. They are also responsible for ensuring that all staff are trained in Data Protection and are aware of their responsibilities.

13.4 Where staff undertake research which involves personal data, they must ensure that it is carried out with reference to Data Protection and ethical guidelines. Where appropriate they must document data retention.

13.5 Staff: All staff or others who process personal data must ensure that they understand their obligations under this Policy and how to protect personal data and that they follow the guidance provided at all times.

13.6 All staff are responsible for reporting any breach or potential incident, likely to result in unauthorised disclosure, damage, destruction or loss of Personal Data directly to the Data Protection Officer.

13.7 Staff/Students as Data Subjects: All staff and students are responsible for:

- checking that any information that they provide to the College is both accurate and up to date, and
- informing the College of any changes to information which they have provided, i.e. changes in addresses, and
- informing the College of any errors in the information it holds about them.

13.8 Data Protection Officer: [[name]] is the appointed Data Protection Officer responsible for the management of data protection matters and for the development of specific guidance and practice on data protection issues for the College. The tasks of the DPO are as follows:

- to inform and advise the College and its employees about their obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR and other data protection laws, and with the College's data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the supervisory authority; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, students etc).

13.9 IT Administrator: The IT Administrator is responsible for ensuring the security of the College's IT systems which enable the processing of personal data by ensuring that there are appropriate technical and organisational security measures in place to protect personal data. S/he is also responsible for maintaining a record of breaches.

14. Authority to Collect Data

14.1 Apart from Central Services, no other Department should routinely be collecting and storing students' personal data except for one off instance such as correspondence, field trips for health, safety purposes and attendance monitoring.

14.2 Managers should only collect staff data as advised by the Human Resources Department.

15. Data Protection Training

15.1 It is mandatory for staff to undertake Data Protection Training. On-line E-Learning Data Protection training and data protection seminars will be held to assist members of staff with an understanding of

their legal duty under the legislation. Staff in key roles will be provided with additional Data Protection training.

15.2 Data Protection training will be a part of a new member of staff's induction.

15.3 Failure to complete any mandatory Data Protection training may give rise to disciplinary action.

16. Data processors

16.1 The college uses data processors, usually to store data and/or operate software on its behalf. Examples include Microsoft and Turnitin. Where it uses a data processor, the College is still responsible for data protection and liable for any data transferred.

16.2 The College is also liable for the data processor's compliance with the legislation and must only appoint processors who can provide sufficient guarantees that the requirements of the legislation will be met and the rights of data subjects protected. It must, therefore, ensure that there is an appropriate written contract with the data processor. The contract is important so that both parties understand their responsibilities and liabilities.

16.3 Contracts must 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 data subject, and the obligations and rights of the controller and which must, as a minimum set out the following:

- only act on the written instructions of the College;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the College and under a written contract;
- assist the College in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the College in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the DPO immediately if it is asked to do something infringing the GDPR or other data protection law of the UK.

17. Documentation

17.1 To comply with the legislation and the requirements for documentation, the College will ensure that it documents the location and retention of all records within the College in a records retention schedule.

17.2 Where consent is used as the lawful basis for processing, records of consent must be retained.

17.3 The College must also document:

- Controller-processor contracts;
- Data Protection Impact Assessment reports;
- Legitimate Interest Assessments
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data, covering: - the condition for processing in the Data Protection Bill - the lawful basis for the processing in the GDPR - the retention and erasure policy document.

18. Security

18.1 The legislation requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

18.2 The IT department in particular is responsible for working with data owners to ensure appropriate security measures are in place.

18.3 All staff are responsible for ensuring personal data are kept securely and accessible only to those who need to use it. Appropriate security measures are to be taken to prevent accidental loss of, or damage to, personal data. This will mean the use of passwords or encryption for electronic documents and keeping papers under lock and key.

18.4 The transport of personal data in any format (laptop, hard copy, memory stick etc.) should be avoided as far as possible. This applies especially to special categories data, large volumes of personal data, or information which could cause particular harm or distress if lost. Only in exceptional circumstances should this information be transported outside of the College. Staff who do so should always ensure that it is kept with them at all times. Staff should:

- Where possible use remote login to their College account to access information as an alternative to transporting data.

- Only carry the minimum amount of personal data (e.g. avoid carrying the whole file if only one document is needed).
- It is the College's intention that all mobile devices (laptops, smartphones, tablets) and external storage media (USB sticks, external hard drives, etc.) used to transport personal data and special categories data outside the College will be secured by deploying strong encryption.

18.5 Any loss/theft must be immediately reported to the DPO this represents a breach of this policy and must be recorded and reviewed for any action required.

18.6 When working remotely staff should:

- Never use unsecured public networks;
- Never save documents containing personal data to a personal PC;
- Consider that the means of connection may not always be secure.

19. International Transfers

19.1 In accordance with the Legislation, the College may not transfer personal data to countries outside of the European Economic Area (EEA) (the European Union Member States along with Iceland, Liechtenstein and Norway) unless the country or territory has an adequate level of protection for personal data.

19.2 There are however a number of non-EEA countries recognised by the European Commission to have adequate level of personal data protection ("approved countries"). Transfer of information to these countries will not breach the Data Protection Legislation. Information on the European Commission's list of approved countries is available on the **Information Commissioners website**.

19.3 The College may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. These adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by ICO and approved by the Commission;

- compliance with an approved code of conduct approved by the ICO;
- contractual clauses agreed authorised by the ICO

19.4 The legislation permits that a transfer, or set of transfers, may also be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The College may not rely on the first three of these reasons when the lawful basis for processing is public task, e.g. for the provision of higher education or research. In these cases therefore, the College must have a provision outlined in 17.3 in place before any transfer is made.

20. Breaches

20.1 All breaches of data protection should be reported to the DPO using the Breach Reporting Process. An assessment will be made as to whether there are significant risks to the rights and freedoms of individuals and whether a notification must be made to the Information Commissioner's Office. Any such notification must be approved by the DPO and reported within 72 hours of the notification of the breach.

20.2 It is essential that staff report a breach or potential breach immediately. This allows quick action to be taken to address the breach, as well as allowing the College to comply with its obligation to report breaches.

20.3 If there has been clear negligence or intent with regard to any breach of the Data Protection Policy by members of staff or students, the College will consider the circumstances and decide how best handle the next steps. Where a staff member has been negligent without mitigation, this will be dealt with in

accordance with the College's disciplinary procedures. All factors will be taken into account when determining appropriate action, including whether the beach was reported promptly.

20.4 In addition, a breach of the Policy may expose the College and individual concerned to criminal or civil liabilities. In addition to any College liability, staff may also personally liable. Data subjects may also apply to court for compensation if they have suffered damage from such a loss.

21. Data Storage, Retention and Disposal

21.1 It is the responsibility of the relevant senior manager to ensure that centralised records are maintained to meet the needs and reasonable expectations of students, the College, and external bodies. For members of staff, Human Resources has the responsibility of ensuring that centralised records are maintained.

21.2 Central databases (such as the Student Records System) should be used to avoid duplication of information and to increase data security. All local databases maintained by staff in the course of their duties containing personal data (including those using reference numbers for individuals rather than names) must be adequately secure.

21.3 The College is required to ensure that all data is accurate and up-to-date. Staff and students have a responsibility to regularly update their records by notifying the College Administration.

21.4 The College should not retain personal data for longer than is necessary. This means that personal data should be destroyed or deleted when it is no longer required.

21.5 Staff should regularly review their records to ensure that the documents they hold are destroyed within the relevant destruction time limit in accordance with the Records Retention Schedule. Where the documentation contains personal information, the destruction must take place confidentially (e.g. shredding, disposal as confidential waste, secure electronic deletion).

22. Disclosure

22.1 Staff must not disclose personal data to a third party except in limited cases where there is a legal or statutory duty to do so or where it is in an individual's vital interests. All staff must therefore take care to ensure that personal data is not disclosed to unauthorised third parties which includes family members of the data subject, friends, government bodies and the Police in certain circumstances without the data subject's consent.

22.2 Where the Police are requesting data, this must be dealt with by the College Secretary on receipt of the required form.

22.3 Where regular disclosures are made (for example to the Local Authorities and Awarding bodies) there must be a documented procedure and the data subject must be informed.

23. Rights of Access

23.1 Staff, students and other data subjects about whom the College holds or uses personal data have a legal right to access that information and request a copy of the data in permanent form. Any person wishing to exercise their right of access formally should complete the "Data Subject Access Form" and submit it along with evidence of proof of identity to prevent unlawful disclosure of personal data to DPO (dpo@seginternationalcollege.com)

23.2 By law, the College has one month from receipt of the request and proof of identity, in which to respond to subject access requests, in any event the College will endeavour to respond as quickly as possible. In limited circumstances, the College may not be able to release personal data because exemptions under the Legislation are applicable, or the disclosure of the data would release personal data relating to other individuals.

23.3 The College is committed to openness and current members of staff may view their personnel file, at no charge, by either making an appointment to visit the Human Resources office or requesting copies of their personnel file.

23.4 Students who wish to access copies of their student files or any other personal data should make a subject access request.

23.5 Staff who receive a request for personal information from an individual (data subject) or a third party acting on behalf of a data subject, they should be directed to the Subject Access Request form.

23.6 Where a third party is acting on behalf of a data subject, written authorisation from the data subject must be provided to confirm that the third party is acting on their behalf.

23.7 All requests should be passed to the DPO where the data subject is seeking information about themselves, even if they do not mention the data protection.

24. Email and Social Media Usage

24.1 Staff should avoid using e-mail to send personal data or to express views about individuals. This is because e-mail is an insecure medium and the sender has no control over the storage or use of the message after it has been sent.

24.2 Staff should only communicate with students using College supported communication tools such as Blackboard. Staff must not communicate with students using social media including Facebook or WhatsApp as the College has no control over these systems.

24.4 The College reserves the right to monitor the use of its e-mail facilities and other internet traffic in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

25. CCTV

25.1 The College operates close circuit television cameras (CCTV) in its premise for the security and safety. The College's use of CCTV must be in compliance with the Data Protection Legislation.

25.2 The College is committed to the protection and security of personal data especially as applied in the use, operation and monitoring of CCTV images. As such:

- All security staff involved in the recording, observation and capture of images must act in an ethical and lawful manner in accordance with legislation and must receive adequate training to ensure their understanding of compliance legislation.
- Only authorised persons involved in the monitoring or investigation can view CCTV images.
- All recorded material will be treated as confidential and unless required for evidence will only be kept in accordance with CCTV policy guidelines.
- CCTV will not be retained for longer than necessary in accordance with the data protection principles.
- Data is stored and managed automatically by the CCTV digital recorders which use software programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces a minimum of 1 month rotation in data retention.

25.3 If CCTV images are retained beyond the retention period, they are to be stored in a secure place to which access is controlled and are to be erased when no longer required.

26 Direct Marketing

26.1 If the College uses personal data for direct marketing purposes, it must inform the data subject of this at the time of collection of the information. The lawful basis of processing will normally be consent and the data subject must be provided with the opportunity to opt in and to object to the use of their data for direct marketing purposes.

26.2 In the case of sending information to enquirers, applicants and alumni, where they would reasonably expect the college to use their data in this way, data may be used to send these individuals electronic communications. They must be provided with a simple way to object to the use of their data in this way in any communication.

26.2 Direct Marketing must also be in line with the Privacy and Electronic Communications Regulations (PECR).

27. Research

27.1 Personal data for research purposes is collected on the basis of public task. Collection of special categories data is on the basis that it is for research purposes. Consent to being part of the research study must still be collected and retained in accordance with the Research Ethics Code of Practice. No collection of data is permissible until ethical approval has been given by the College Research Ethics Committee.

27.2 Personal data collected for research purposes must not be used in forming any decisions about a particular individual and must not be used in any way that will, or is likely to, cause distress to any data subject.

27.3 The research data should be anonymised as soon as possible. It should be retained in accordance with the Research Data Management Statement.

Data Subject Access Form

Part 1 – About Yourself

SURNAME:

FIRST NAME(S):

ID NUMBER:

CURRENT ADDRESS:
(including postcode)

PHONE NUMBER:

EMAIL ADDRESS:

DATE OF BIRTH:

Part 2 - Locating Your Personal Information

In order for us to be able to locate the information you are seeking, please provide some details, if known, as to where you feel information is held about you.

SUBJECT DETAILS:

You may continue on plain sheets if necessary

Part 3 – Confirming Your Identity

In line with Article 12(6) of the GDPR, we will require additional information to enable identification.

Please provide proof of postal address and identification. For identity purposes please send a copy of **one** of the following documents listed below. Hard copies of documents will be returned once the search is completed.

- Photocopy of passport
- Photocopy of Driver's License

Proof of postal address can include:

- Original of electricity bill
- Original of gas bill
- Original council tax bill
- Original of any other bill in your full name
- Bills should not be more than six months old

Part 4 - Declaration

Please read the following declaration carefully and sign and date it.

I, ... certify that the information provided on this application to SEG International College is true. I understand that it is necessary for the College to confirm the data subject's identity and that it may be necessary for the College to request more details from me in order to be able to locate the correct information.

Signature: …… Date: ……

Please email the completed form and the identity documents to:

dpo@seginternationalcollege.com