Policy:	Data Protection Policy	
Synopsis:	This policy sets out the principles and legal conditions that Study Group must satisfy when obtaining, handling, processing, transporting or storing personal data in the course of operations and activities, including student and employee data.	
Authority	The Global Executive Team	
Policy Owner:	The Data Protection Officer	
Relevant to:	All Study Group employees including workers, contractors, consultants and agency workers.	
Publication:	March 2026	
Next review date:	March 2028	
Related Document:	Study Group Global Code of Conduct Study Group Disciplinary Policy Study Group CCTV Policy	
Version Control	**Date Issued**	**Next Review**
1.0	June 2017	April 2018
2.0	April 2018	April 2019
3.0	April 2019	April 2020
4.0	May 2020	May 2022
5.0	July 2022	July 2024
6.0	March 2026	March 2028

POLICY STATEMENT

As an acknowledged leader in international education, Study Group recognises its long standing ethical and regulatory responsibilities to act in accordance with applicable data protection laws and regulations in all of our global locations in which we operate.

Study Group is committed to acting professionally, fairly and with integrity in all of our business dealings and relationships wherever we operate. We commit to implementing and enforcing effective systems to ensure data is processed in accordance with the relevant laws and regulations.

Study Group will uphold all laws and regulations relevant to data protection in all jurisdictions in which we operate.

1. DEFINITIONS:

Agents: third party recruitment agents who refer students to Study Group.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing which produces legal effects or significantly affects an individual.

Automated Processing: any form of automated processing of Personal Data to evaluate personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Company: SG Topco Limited and all subsidiaries and otherwise affiliated companies.

Company Personnel: employees, contractors, consultants, agency workers, Agents, Homestay providers and family members, Study Group University Partners, accommodation providers, students, medical professionals, and third party contractors**.** Unless otherwise agreed, these persons are deemed to be persons acting under the authority of the Company.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. Study Group UK Limited is the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and

should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): Aphaia Limited who can be contacted at DPO@Aphaia.co.uk.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Homestay Providers: individuals or families who provide accommodation to students.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notice setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

a. general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or
b. Stand-alone, one time privacy statements covering processing related to a specific purpose

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data as stated in the Global and Regional Policies section of the People Hub.

Remote Working: working from any location in which you are not connected directly to a Company server (i.e. home, hotel, etc).

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health

conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Criminal Convictions Data.

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

2. INTRODUCTION

2.1 This Data Protection Policy ("this Policy") sets out how Study Group ("we", "our", "us", "the Company") handle the Personal Data of Company Personnel, customers, prospective customers, suppliers, business contacts and other third parties.

2.2 This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present Company Personnel, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

2.3 This Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. Data protection is the responsibility of everyone within The Company and this Policy sets out what we expect from you when handling Personal Data to enable The Company to comply with applicable law. Your compliance with this Policy is mandatory.

2.4 Related Policies and Privacy Notices are available to help you interpret and act in accordance with this Policy. The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against The Company. You must also comply with all such Related Policies. Any breach of this Policy may result in disciplinary action in accordance with The Company's Disciplinary Policy.

2.5 Where you have a specific responsibility in connection with Processing, such as capturing Consent, reporting a Personal Data Breach or conducting a DPIA as referenced in this Policy or otherwise, then you must comply with the Related Policies.

2.6 This Policy (together with Related Policies) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer (DPO).

3. SCOPE

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain trust and confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of our total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the UK GDPR.

3.2 All of The Company's Board members, Executive Committee members via business areas and line managers are responsible for ensuring all Company Personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3 The DPO is responsible for monitoring compliance with this Policy and to facilitate appropriate practices, processes, controls and training to ensure such compliance. The DPO can be contacted at dpo@aphaia.co.uk or through a member of the legal team at privacy@studygroup.com.

3.4 The DPO is also responsible for overseeing this Policy and, as applicable, developing Related Policies.

3.5 Please contact the DPO with any questions about the operation of this Policy or the UK GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company);

(b) if you need to rely on Consent and/or need to capture Explicit Consent;

(c) if you need to draft Privacy Notices;

(d) if you are unsure about the retention period for the Personal Data being Processed;

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data;

(f) if there has been a Personal Data Breach;

(g) if you are unsure on what basis to transfer Personal Data outside the UK;

(h) if you need any assistance dealing with any rights invoked by a Data Subject;

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;

(k) If you need help complying with applicable law when carrying out direct marketing activities; or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given their Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations.;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. ‘Legitimate interests’ should be interpreted narrowly, and a legitimate interest test is required in cases of new types of processing on this basis. The purposes for which we process Personal Data based on legitimate interests need to be set out in applicable Privacy Notices.

5.4 You must identify and document the legal ground being relied on for each Processing activity.

6. CONSENT

6.1 A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent.

6.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.4 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Categories of Personal Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

6.5 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies so that the Company can demonstrate compliance with Consent requirements.

7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

7.1 The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a notice which must be presented when the Data Subject first provides the Personal Data. Notices used for students and employees respectively can be provided on request.

7.3 When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the UK GDPR as

soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7.4 You must comply with the Company's guidelines on drafting Privacy Notices.

8. CLOUD PROVIDERS

8.1 Where The Company uses Cloud services, we retain responsibility as the Data Controller for any data it puts into the service and can consequently be fined for any Personal Data Breach, even if this is the fault of the Cloud service provider. The Company will also bear the responsibility for contacting Information Commissioner's Office concerning the Personal Data Breach, as well as any affected individual. To ensure we have provided adequate measures to prevent a Personal Data Breach we have the following stipulations:

(a) Cloud services used to process personal data will be expected to have ISO27001 or similar certification, or otherwise being able to demonstrate information security, with adherence to the standard considered the best way of a supplier proving that it has met the UK GDPR principle of privacy by design, and that it has considered information security throughout its service model. Any request for exceptions will be considered by the DPO.

(b) Cloud providers must be subject to a data processing agreement that complies with Article 28 UK GDPR and, where based in third countries, standard contractual clauses.

9. PURPOSE LIMITATION

9.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

9.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

9.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this Policy.

10. DATA MINIMISATION

10.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

10.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

10.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

10.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with The Company's retention guidelines.

11. ACCURACY

11.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. Data Subjects have the right to have any errors rectified.

11.2 You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

12. STORAGE LIMITATION

12.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

12.2 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

12.3 The Company will maintain retention policies, including a global retention schedule, and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

12.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer. This includes requiring third parties to delete such data where applicable.

12.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

13. REMOTE WORKING

13.1 When Remote Working you will be utilising Company provided devices or your personal devices. You must only store data on Company devices or on Company approved cloud storage providers (i.e. Study Group Dropbox or Study Group OneDrive). You must use VPN when accessing

Company systems remotely and you must not store any Company data on your personal devices or on cloud storage providers that have not been approved by the Company.

13.2 You will uphold reasonable standards of security at all times (i.e. by ensuring that you leave your devices locked (e.g. Windows Key + L) when not in use and by ensuring any hard copy documents are locked away in storage when not required.

13.3 Any loss or theft of a device used for Remote Working must be reported immediately as a potential Personal Data Breach in accordance with section 16 of this Policy.

13.4 If you have any queries regarding your data protection obligations whilst Remote Working , please contact the legal team at privacy@studygroup.com.

14. INFORMATION SECURITY, INTEGRITY AND CONFIDENTIALITY

14.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

14.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

14.3 You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

14.4 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and to protect Personal Data from the point of collection to the point of destruction

14.5 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. See also the chapter on Cloud Providers.

14.6 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

14.7 You must ensure that you handle Personal Data in accordance with its classification level and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities. The following information classifications have been adopted by us which underpin the principles of information security:

Security Level	Definition	Examples	FOIA2000 exemption
1. Confidential	Normally accessible only to specified members of Study Group employees. Should be stored in an encrypted state or with appropriate security safeguards;	Sensitive Personal Data *(*which includes racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record) passwords; large aggregates of personally identifying data (>1000 records) including elements such as name, address, telephone number.	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
2. Restricted	Normally accessible only to specified members of Study Group employees	Personal Data which is information that identifies living individuals including home addresses, age, telephone number, schools attended, photographs, grades attained);	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
3. Internal Use	Normally accessible only to members of Study Group staff and the student body	Communications between employees where intended for a wider circle of recipients, decisions about students being admitted,	Subject to scrutiny in relation to appropriate exemptions/ public interest and legal considerations
4. Public	Accessible to all members of the public	Annual accounts, minutes of statutory and other formal committees, Information available on the Study Group website or through the	Freely available on the website or through the Study Group's Publication Scheme.

		Study Group's Publications.	

15. MONITORING OF EMPLOYEE ACTIVITIES

15.1 Monitoring of emails and other online or offline activities may be undertaken where proportionate in order to prevent or investigate abuse of students or staff, the leaking of confidential information or neglect of duties in the course of employment.

15.2 Where such monitoring is undertaken, it shall be under permission of the senior management and duly documented.

16. REPORTING A PERSONAL DATA BREACH

16.1 The GDPR requires Data Controllers to notify certain Personal Data Breaches to the applicable regulator and, in certain instances, the Data Subject.

16.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

16.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact your line manager and the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

17. TRANSFER LIMITATION

17.1 The UK GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

17.2 You must comply with the Company's guidelines on cross-border data transfers.

17.3 You may only transfer Personal Data outside the UK if one of the following conditions applies:

(a) the UK has issued regulations confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO. Note that Study Group uses standard contractual clauses for intra-group transfers;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

18. DATA SUBJECT'S RIGHTS AND REQUESTS

18.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities and request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

(c) request rectification of inaccurate or incomplete data;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data. In case of any published data, this may require us to ask the same from other data controllers who make the same data available online;

(f) restrict Processing in specific circumstances – which may require DPO's advice;

(g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the relevant supervisory authority (e.g. the Information Commissioner's Office in the UK); and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

18.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

18.3 You must immediately forward any Data Subject request you receive to the DPO.

19. THE COMPANY'S ACCOUNTABILITY

19.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

19.2 The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a suitably qualified DPO and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing might present a high risk to rights and freedoms of Data Subjects and/or this is required by UK GDPR or the ICO guidance;

(c) integrating data protection into internal documents including this Policy, Related Policies and Privacy Notices;

(d) regularly training Company Personnel on the UK GDPR, this Policy, Related Policies and Privacy Notices and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

20. RECORD KEEPING

20.1 The UK GDPR requires us to keep full and accurate Record of all our data Processing activities.

20.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

20.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows. Any such records must be reflected in Study Group's central Record of Processing Activities (RoPA).

21. TRAINING AND AUDIT

21.1 We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

21.2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

21.3 You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

22. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

22.1 We are required to implement privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

22.2 You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing. To assess whether a DPIA is required, there is a DPIA Screener to help you. If you answer any of the questions on the DPIA Screener with a 'yes' then a DPIA is required.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(e) use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes);

(f) Automated Processing including profiling and ADM;

(g) large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

(h) large scale, systematic monitoring of a publicly accessible area.

22.3 To help you assess whether a DPIA is required, there is a DPIA Screener to help you. If you answer any of the questions on the DPIA Screener with a 'yes' then a DPIA is required.

22.4 A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

23. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

23.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

23.2 If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed. However, the Special Categories of Personal Data or Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

23.3 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

23.4 We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

23.5 A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

23.6 Where you intend to use any generative AI tool, you must comply with the Company's policy on generative artificial intelligence in the workplace.

24. DIRECT MARKETING

24.1 We are subject to certain rules and privacy laws when marketing to our customers.

24.2 For example, a Data Subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message. For example we may send communication to existing students' informing them of alumni events or future courses of interest.

24.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information. In principle, it should be a one-click option on each email sent, or any such statement made during a call.

24.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

24.5 You must comply with the Company's guidelines on direct marketing to customers and you should consult your line manager **or** the DPO if you are unsure regarding how to comply with either the Company's guidelines or the law.

25. SHARING PERSONAL DATA

25.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

25.2 You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

25.3 You may only share the Personal Data we hold with an, employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information, which is compatible with the purpose of the data being collected, and the transfer complies with any applicable cross-border transfer restrictions.

25.4 You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services, which is compatible with the purpose of the data being collected;

(b) they have a legal right to obtain such data as data controllers or recipients, or we have with them a data processor agreement in place (can be governed by their standard terms) or a fully executed written contract that contains UK GDPR-compliant third party clauses; - see also the chapter on Cloud Providers;

(c) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(d) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and

(e) the transfer complies with any applicable cross border transfer restrictions.

26. CHANGES TO THIS POLICY

26.1 This Policy is kept under regular review. The Policy will always be accessible to our employees and other Company Personnel.

26.2 This Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates. Certain countries may have localised variances to this Policy which are available upon request to the DPO.

26.3 If you have any queries related to this policy, please contact the legal team at privacy@studygroup.com or the DPO at dpo@aphaia.co.uk.