General Data Protection Regulation (GDPR) Policy

London Professional College
First Floor, Moorfoot House
221 Meridian Pl, Marsh Wall
London E14 9FJ

Phone: +44 (0) 20 3621 2479
Email: info@londonpc.org.uk
Web: www.londonpc.org.uk

Version : 1.23
Last Updated : 5 February 2024

Table of Contents

General Data Protection Regulation (GDPR) Policy

1. Introduction

London Professional College (referred to as "the College") acknowledges the significance of data protection and privacy in the digital age. As an institution dedicated to providing higher education diplomas and courses, the College recognises its responsibility to safeguard the personal data of students, staff, and any individuals associated with its operations.

1.1 Purpose

The purpose of this GDPR policy is to establish a framework that ensures the lawful, fair, and transparent processing of personal data by the College and its external agents. This policy outlines the principles and procedures that guide the collection, processing, and protection of personal data, in strict adherence to the General Data Protection Regulation (GDPR) and other relevant data protection laws.

1.2 Scope

This policy applies to all personal data processed by the College, whether collected directly from individuals or received from external agents. It encompasses data related to students, employees, contractors, and any other individuals whose data is handled in the course of the College's activities.

1.3 Commitment to Compliance

The College is committed to upholding the principles of data protection, respecting individual privacy rights, and ensuring compliance with applicable data protection laws. This commitment extends to all staff, external agents, and stakeholders involved in the processing of personal data on behalf of the College.

1.4 Legal Basis for Processing

The College will only process personal data when there is a lawful basis for doing so, as defined by the GDPR. This includes obtaining explicit and informed consent when required, fulfilling contractual obligations, complying with legal obligations, protecting vital interests, performing tasks carried out in the public interest, or pursuing legitimate interests that are not overridden by the rights and interests of data subjects.

1.5 Data Protection Officer (DPO)

The College has appointed a Data Protection Officer responsible for overseeing compliance with this policy and related data protection matters. The DPO serves as a point of contact for data subjects and supervisory authorities.

1.6 Review and Revision

This GDPR policy will be regularly reviewed and, if necessary, revised to ensure its ongoing relevance and compliance with changes in legislation, College operations, and best practices in data protection.

In adopting this GDPR policy, the College affirms its dedication to maintaining the highest standards of data protection and privacy, fostering trust among stakeholders and contributing to a secure and ethical information environment.

2. Data Processing Agreement (DPA)

2.1 Overview

External agents, including self-employed freelancers acting as referrers, play a crucial role in the admission process of London Professional College. To ensure the secure and lawful processing of personal data on behalf of the College, all external agents must enter into a formal Data Processing Agreement (DPA).

2.2 Purpose of the DPA

The Data Processing Agreement outlines the specific obligations and responsibilities of external agents regarding the collection, processing, and sharing of personal data. It serves as a legally binding document that ensures external agents adhere to the same high standards of data protection as the College.

2.3 Key Components of the DPA

The DPA includes, but is not limited to, the following key components:

- **Data Processing Purpose:** Clearly defined purposes for which personal data is collected and processed.
- **Data Types:** Specification of the types of personal data that may be processed by external agents.
- **Confidentiality and Security Measures:** Requirements for maintaining the confidentiality and security of the processed data, including encryption and secure transmission methods.
- **Data Subject Rights:** Recognition and support for the rights of data subjects, including the right to access, rectification, erasure, and restriction of processing.
- **Subcontracting:** Restrictions and conditions on subcontracting the processing of data to third parties.
- **Data Breach Notification:** Procedures for notifying the College of any data breaches without undue delay.

2.4 Compliance Assurance

External agents must provide assurances of compliance with the DPA and GDPR principles. This may involve regular reporting, audits, and documentation of their data processing activities.

2.5 Termination of Agreement

Provisions for the termination of the DPA in the event of non-compliance, ensuring that the College can swiftly address any breaches of data protection obligations.

2.6 DPA Training

External agents will receive training on the contents and implications of the DPA to ensure a clear understanding of their responsibilities and obligations.

2.7 Legal Review

External agents are encouraged to seek independent legal advice before entering into the DPA to ensure a full understanding of their legal obligations and responsibilities.

The College is committed to fostering a collaborative relationship with external agents while upholding the highest standards of data protection. Through the implementation of the Data Processing Agreement, the College aims to establish a framework that not only ensures legal compliance but also instils confidence in the individuals whose data is entrusted to external agents in the course of the admission process.

3. Training and Awareness

3.1 Training Programs

London Professional College recognises the critical role that all individuals involved in the processing of personal data play in maintaining compliance with GDPR principles. To ensure a high level of awareness and understanding of data protection obligations, the College has established comprehensive training programs for all staff and external agents.

3.2 Training Content

The training programs cover the following key areas:

- **GDPR Principles:** A detailed explanation of the fundamental principles of the General Data Protection Regulation, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

- **Data Subject Rights:** An overview of the rights of individuals regarding their personal data, including the right to access, rectification, erasure, and the right to object to processing.

- **Secure Data Handling:** Best practices for the secure collection, processing, storage, and transmission of personal data, emphasising the use of encryption and secure communication channels.

- **Consent Management:** Guidance on obtaining and managing explicit and informed consent for data processing activities.

- **Data Breach Response:** Protocols for identifying, reporting, and responding to data breaches in compliance with GDPR requirements.

3.3 Frequency of Training

Training sessions are conducted regularly, ensuring that all staff and external agents remain up-to-date with any changes in data protection laws, regulations, or internal policies. New staff and external agents will undergo data protection training as part of their onboarding process.

3.4 Accountability and Responsibility

Individuals processing personal data are accountable for their actions, and the training programs emphasise the importance of individual responsibility in maintaining GDPR compliance. This includes an understanding of the consequences of non-compliance, both for individuals and for the College.

3.5 Assessment and Certification

At the conclusion of training programs, participants may undergo assessments to evaluate their understanding of GDPR principles. Certification may be provided upon successful completion of these assessments, serving as a record of participation and competence.

3.6 Ongoing Awareness Campaigns

To maintain a culture of data protection awareness, the College conducts ongoing awareness campaigns, which may include regular communications, reminders, and updates on emerging trends or changes in data protection legislation.

The College believes that a well-informed and trained workforce is essential for upholding the principles of data protection. By investing in comprehensive training and awareness initiatives, the College aims to foster a culture of data protection consciousness among its staff and external agents, thereby ensuring the secure and lawful processing of personal data.

4. Explicit Consent

4.1 Importance of Consent

London Professional College recognises the significance of obtaining explicit and informed consent for the collection, processing, and sharing of personal data. Consent is a fundamental principle of GDPR and serves as the legal basis for processing in many instances.

4.2 Consent Collection Process

- **Clear and Unambiguous Language:** Consent will be sought using clear and unambiguous language, avoiding any ambiguity or misleading statements. Individuals will be fully informed about the purpose of data collection and processing.

- **Separate Consent for Each Purpose:** Consent will be obtained separately for each specific purpose of data processing, ensuring that individuals have a clear understanding of the intended use of their data.

- **Withdrawal of Consent:** Individuals will be informed of their right to withdraw consent at any time. The process for withdrawing consent will be clearly communicated, and the withdrawal will be respected without any adverse consequences.

4.3 Consent Records

- **Documenting Consent:** The College will maintain records of obtained consents, including the time, date, and the specific information provided to individuals at the time of obtaining consent.

- **Regular Review of Consent Records:** Consent records will be regularly reviewed to ensure that consents remain valid and relevant. If there are changes in data processing activities, individuals will be informed, and new consents may be obtained.

4.4 Age Verification for Minors

Age Verification Measures: In cases where the processing of personal data involves individuals below the age of 16, the College will implement age verification measures to ensure that consent is obtained from a parent or guardian.

4.5 Alternatives to Consent

Legal Basis for Processing: Where consent is not the most appropriate legal basis for processing personal data, the College will identify and rely on alternative legal bases as provided for in the GDPR.

4.6 Communication of Consent Procedures

Clear Communication: The procedures for obtaining and managing consent will be clearly communicated to individuals through privacy notices, consent forms, and any other relevant channels.

Language Accessibility: Efforts will be made to ensure that consent procedures and information are accessible to individuals with varying levels of language proficiency.

4.7 Periodic Consent Reviews

The College will conduct periodic reviews of its consent processes to ensure ongoing compliance with GDPR requirements. This may include updating consent forms, revising procedures, and implementing improvements based on feedback and developments in data protection practices.

London Professional College is committed to ensuring that the processing of personal data is founded on the explicit and informed consent of individuals. By implementing robust consent procedures and regularly reviewing and improving these processes, the College aims to uphold the principles of transparency, fairness, and accountability in its data processing activities.

5. Data Minimisation

5.1 Principle of Data Minimisation

London Professional College is committed to the principle of data minimisation, ensuring that only the necessary personal data required for the admission process is collected, processed, and retained. This principle aligns with the GDPR requirement to limit the processing of personal data to what is strictly relevant and essential for the intended purpose.

5.2 Specific Data Collection Purposes

Admission Process: The College will only collect personal data that is directly relevant and necessary for the admission process. This includes information such as contact details, educational qualifications, and other details required for academic evaluation.

Commission-related Information: External agents collecting data for commission purposes will be provided with clear guidelines on the specific information required for commission calculations, limiting the collection to what is strictly necessary for this purpose.

5.3 Avoidance of Excessive Data

Exclusion of Unnecessary Information: Unnecessary or excessive information will be actively excluded from the data collection process. This includes sensitive information that is not directly relevant to the admission or commission processes.

Regular Data Audits: The College will conduct regular audits to ensure that the data collected remains in line with the principle of data minimization. Any outdated or no longer necessary information will be promptly identified and securely disposed of.

5.4 Periodic Data Reviews

Data Review Committees: The College may establish data review committees tasked with assessing the necessity of data collected for various purposes. These committees will ensure ongoing compliance with data minimization principles.

5.5 Consent for Additional Processing

Explicit Consent for Additional Data Processing: In cases where additional data processing is necessary beyond the initial admission or commission purposes, explicit consent will be sought from the individuals concerned. The purpose and scope of the additional processing will be clearly communicated.

5.6 Data Minimization in Commission Calculations

Commission-related Data Minimization: External agents involved in commission-related activities will be instructed to collect only the data required for commission calculations. Unnecessary personal information will not be requested or processed.

5.7 Education and Awareness Programs

Training for Data Handlers: Staff and external agents involved in data collection processes will undergo training on the principles of data minimization. This training will emphasize the importance of collecting only the data that is strictly necessary for the intended purpose. London Professional College considers data minimization as a fundamental aspect of its commitment to data protection and privacy. By actively limiting the collection and processing of personal data, the College aims to reduce privacy risks, enhance data security, and uphold the trust placed in its data handling practices by students, staff, and external agents.

6. Secure Data Transmission

6.1 Importance of Secure Data Transmission

London Professional College places a paramount emphasis on the secure transmission of personal data. The confidentiality and integrity of this data are critical components of the College's commitment to GDPR compliance and the protection of individuals' privacy.

6.2 Encrypted Communication Channels

Use of Encryption: To ensure the security of data in transit, the College mandates the use of encrypted communication channels for the transmission of sensitive information. This includes, but is not limited to, personal details, academic records, and any other data exchanged between external agents and the College.

Secure Email Communication: External agents are encouraged to use secure email communication protocols when transmitting personal data. This includes the use of encryption technologies to safeguard the contents of emails containing sensitive information.

6.3 Secure Data Storage Measures

Secure Data Storage: In addition to secure transmission, the College implements robust measures for the secure storage of personal data. This involves the use of secure servers, access controls, and encryption technologies to protect the data from unauthorized access or breaches.

Access Controls: Access to personal data is restricted to authorised personnel only. Access controls are implemented to ensure that individuals can only access the data necessary for their specific role, thereby minimising the risk of unauthorised disclosure.

6.4 Data Encryption Guidelines for External Agents

External agents are provided with clear guidelines on the encryption of data during transmission. This includes instructions on the use of secure and encrypted platforms or services when submitting personal information to the College.

6.5 Regular Security Audits

To maintain the highest standards of data security, the College conducts regular security audits. These audits include assessments of data transmission and storage practices to identify and address any potential vulnerabilities or areas for improvement.

6.6 Data Breach Response Plan

Despite stringent security measures, the College acknowledges the possibility of data breaches. In the event of a data breach, a comprehensive response plan is in place, outlining the steps to be taken to mitigate the impact of the breach and ensure timely reporting to relevant authorities and affected individuals.

6.7 Continuous Improvement

Feedback Mechanisms: The College encourages a culture of continuous improvement in data security. Feedback mechanisms, including incident reporting systems and employee or agent feedback, are established to identify areas for enhancement in data transmission and storage practices.

In prioritising secure data transmission, London Professional College is committed to maintaining the trust of individuals associated with its operations. By implementing and regularly reviewing these measures, the College aims to protect the confidentiality and integrity of personal data and respond effectively to any potential security challenges.

7. Data Security Measures

7.1 Commitment to Robust Data Security

London Professional College recognises the paramount importance of maintaining the confidentiality, integrity, and availability of personal data. The College is committed to implementing and upholding robust data security measures to protect against unauthorised access, disclosure, alteration, and destruction of personal information.

7.2 Secure Data Storage Practices

Secure Servers: The College employs secure servers with industry-standard security protocols to store personal data. These servers are maintained in controlled environments with restricted access to authorised personnel only.

Access Controls: Access controls are implemented to ensure that only individuals with the necessary authorisation can access personal data. The principle of least privilege is applied to limit access to the minimum necessary for specific job roles.

7.3 Encryption of Personal Data

All personal data, both in transit and at rest, is subject to encryption. This includes the use of encryption algorithms to convert sensitive information into a secure format, making it unreadable to unauthorised entities.

7.4 Regular Security Audits and Assessments

Periodic Security Audits: The College conducts regular security audits and assessments to evaluate the effectiveness of data security measures. This includes testing for vulnerabilities, assessing the adequacy of access controls, and ensuring compliance with established security protocols.

External Security Audits: Independent external audits may be periodically conducted to provide an objective evaluation of the College's data security practices. This ensures that the College maintains a high level of security and stays abreast of evolving security standards.

7.5 Employee Training on Data Security

All employees, including external agents involved in data processing, undergo comprehensive training on data security practices. Training covers the secure handling of personal data, the importance of confidentiality, and the role of each individual in maintaining data security.

7.6 Incident Response Plan

Despite robust preventive measures, the College acknowledges the possibility of security incidents. An incident response plan is in place to guide the swift and effective response to any data security breaches. This includes procedures for containment, investigation, communication, and recovery.

7.7 Continuous Improvement in Data Security

The College actively encourages a culture of continuous improvement in data security. Feedback mechanisms, incident reporting channels, and employee suggestions are valued as opportunities for identifying and addressing potential weaknesses in the data security framework.

7.8 Compliance with Industry Standards

The College is committed to aligning its data security practices with industry standards and best practices. This commitment includes staying informed about emerging threats and proactively implementing measures to address new security challenges.

London Professional College regards the implementation of robust data security measures as fundamental to maintaining the trust of individuals whose personal data is processed. By continuously assessing and improving its security practices, the College aims to uphold the highest standards of data protection and ensure the confidentiality and integrity of personal information.

8. Audit and Monitoring

8.1 Overview

London Professional College is dedicated to the continuous monitoring and auditing of its data protection practices to ensure ongoing compliance with GDPR regulations and other relevant data protection laws. This section outlines the procedures in place to assess, review, and improve data processing activities.

8.2 Regular Data Audits

Purpose of Data Audits: The College conducts regular internal data audits to assess the compliance of its data processing activities with GDPR principles. These audits include a thorough examination of data collection, storage, and processing practices, as well as the effectiveness of implemented security measures.

Audit Frequency: Internal data audits are conducted at regular intervals, with the frequency determined by the scale and nature of data processing activities. These audits serve as a proactive measure to identify and rectify any potential non-compliance issues.

8.3 External Audits and Assessments

Independent Evaluations: To gain an objective assessment of its data protection practices, the College may engage external entities to conduct independent audits and assessments. This provides an unbiased evaluation of the effectiveness of implemented measures and helps identify areas for improvement.

Adherence to Industry Standards: External audits also ensure that the College's data protection practices align with industry standards and best practices, providing additional assurance to stakeholders and demonstrating a commitment to maintaining high standards of data security.

8.4 Monitoring Data Processing Activities

The College maintains a system of continuous monitoring of data processing activities. This includes real-time monitoring of access logs, data transfers, and other relevant metrics to promptly identify and address any unusual or potentially non-compliant activities.

8.5 Compliance Checks with Data Processing Agreements

The College conducts regular checks to ensure that external agents are complying with the terms outlined in the Data Processing Agreements (DPAs). This involves reviewing the activities of external agents to verify adherence to GDPR principles and the specific obligations outlined in the DPAs.

8.6 Data Subject Rights Monitoring

The College monitors and ensures the effective facilitation of data subject rights. This includes the right of individuals to access their personal data, request corrections, and exercise other rights granted under the GDPR. Any requests received are processed promptly and in accordance with the law.

8.7 Feedback Mechanisms and Continuous Improvement

Feedback Channels: The College actively encourages the use of feedback channels for reporting potential non-compliance, security incidents, or areas for improvement. This includes anonymous reporting mechanisms to foster an open and transparent culture regarding data protection.

Continuous Improvement Initiatives: Feedback received is utilised as input for continuous improvement initiatives. The College is committed to addressing identified weaknesses, enhancing procedures, and adapting to changes in the regulatory landscape to ensure a robust and evolving data protection framework.

8.8 Documentation of Audit Results

The results of internal and external audits, compliance checks, and monitoring activities are comprehensively documented. This documentation serves as a record of adherence to data protection practices and provides a basis for making informed decisions for improvements.

By consistently auditing and monitoring its data protection practices, London Professional College aims to not only meet regulatory requirements but also foster a culture of accountability, transparency, and continuous improvement. These efforts are essential in maintaining the trust of individuals whose data is processed and demonstrating a commitment to the highest standards of data protection.

9. Data Retention Policy

9.1 Importance of a Data Retention Policy

London Professional College recognises the significance of establishing a clear and transparent data retention policy. This policy governs the duration for which personal data is retained, ensuring that data is not held for longer than necessary for the purposes for which it was collected.

9.2 Purpose of Data Retention

Legal Compliance: The data retention policy is designed to ensure legal compliance with GDPR regulations, including the principle of storage limitation. This principle stipulates that personal data should only be kept for as long as is necessary for the purpose for which it was collected.

Minimising Privacy Risks: By adhering to a structured data retention policy, the College aims to minimise privacy risks associated with the unnecessary storage of personal information. This includes reducing the potential for unauthorised access, data breaches, and mitigating the impact of any such incidents.

9.3 Definition of Data Retention Periods

Identification of Retention Periods: The data retention policy clearly defines specific retention periods for different categories of personal data. These periods are determined based on the nature of the data, the purpose of processing, and any legal requirements governing the retention of specific information.

Regular Review and Update: Retention periods are subject to regular review and update to ensure ongoing relevance. Changes in legislation, the nature of data processing activities, or the College's operational requirements may prompt adjustments to retention periods.

9.4 Data Disposal Procedures

Secure Data Disposal:
At the end of the defined retention periods, personal data is securely disposed of using industry-standard practices. This may involve the permanent deletion of digital records or the secure destruction of physical records to prevent unauthorised access.

Documentation of Disposal:
All data disposal activities are documented, including the methods used and the date of disposal. This documentation provides a clear record of compliance with the data retention policy.

9.5 Exceptions and Legal Obligations

Exceptions to Retention Periods:
The policy outlines any exceptions to the standard retention periods, specifying situations where data may be retained for longer periods due to legal obligations, ongoing legal proceedings, or other legitimate reasons.

9.6 Training on Data Retention Policies

All staff and external agents involved in data processing receive training on the data retention policy. This training ensures a consistent understanding of the importance of adhering to retention periods and the secure disposal of data.

9.7 Continuous Review and Improvement

The data retention policy is subject to periodic review to ensure its effectiveness and alignment with evolving legal and operational requirements. Any necessary updates are made to reflect changes in the data protection landscape.

By implementing a robust data retention policy, London Professional College aims to uphold the principles of data protection, ensuring that personal data is managed responsibly, securely, and in compliance with legal requirements. This policy not only protects the privacy of individuals but also contributes to the College's commitment to ethical and lawful data processing practices.

10. Incident Response and Breach Notification

10.1 Incident Identification and Reporting

Internal Reporting Procedures:
The College maintains robust internal reporting procedures for identifying and reporting data security incidents promptly. This includes clear channels for reporting incidents to the designated Data Protection Officer (DPO).

10.2 Data Breach Notification

Timely Notification:
In compliance with GDPR requirements, the College has established procedures for notifying the Information Commissioner's Office (ICO) and affected individuals in the event of a data breach. Notifications are made without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

11. Accountability and Record-Keeping

11.1 Accountability Measures

London Professional College actively demonstrates its commitment to GDPR compliance through accountability measures. This includes maintaining comprehensive records of data processing activities, risk assessments, and the implementation of appropriate safeguards.

11.2 Data Protection Impact Assessments (DPIAs)

Risk Assessments for High-Risk Processing:
Where applicable, the College conducts Data Protection Impact Assessments (DPIAs) for high-risk processing activities. DPIAs help identify and mitigate privacy risks associated with specific data processing operations.

12. Online Class Video Recordings

12.1 Purpose of Video Recordings

Educational Purposes:
London Professional College may record online classes for educational purposes, including facilitating remote learning, providing resources for students, and ensuring the quality of instruction.

12.2 Data Categories Recorded

Participant Data:
Online class video recordings may include the visual and audio data of participants, including students, instructors, and any other individuals present during the session.

12.3 Informed Consent for Recording

Explicit Consent:
Participants in online classes will be informed in advance of any video recording activities. Explicit consent will be sought before initiating video recordings, clearly outlining the purpose of recording and how the recordings will be used.

Withdrawal of Consent:
Participants have the right to withdraw their consent for video recording at any time. The process for withdrawing consent will be clearly communicated, and individuals can choose not to appear on camera if they do not wish to be recorded.

12.4 Data Security Measures

Secure Storage:
Recorded video content will be securely stored, following the data security measures outlined in Section 7 of this GDPR policy. Access controls, encryption, and secure servers will be employed to protect the confidentiality and integrity of the recordings.

Limited Access:
Access to video recordings will be restricted to authorised personnel only, including instructors and relevant administrative staff. The principle of least privilege will be applied to limit access to the recordings to those who require it for educational or administrative purposes.

12.5 Retention Period for Recordings

Defined Retention Period:
The retention period for online class video recordings will be clearly defined in accordance with the data retention policy outlined in Section 9. Recordings will only be retained for as long as necessary for the educational purposes for which they were collected.

12.6 Access Requests for Recordings

Data Subject Access Requests:
Individuals who have been recorded in online classes have the right to request access to the recordings in which they appear. Such requests will be handled in accordance with Section 13 of this policy, addressing data subject rights.

12.7 Data Protection Impact Assessment (DPIA)

Risk Assessment:
Before implementing online class video recordings, a Data Protection Impact Assessment (DPIA) will be conducted to assess and mitigate privacy risks associated with the processing of visual and audio data.

12.8 Communication with Participants

Transparency:
London Professional College is committed to transparent communication with participants regarding the use of video recordings in online classes. This includes providing information about the purpose, consent process, and data protection measures in place.

12.9 Continuous Review and Improvement

The College encourages feedback from participants regarding the use of video recordings in online classes. Feedback will be considered in the continuous review and improvement of practices to enhance privacy protections and educational experiences.

13. Referrals and External Agents

13.1 Engagement with External Agents

London Professional College may engage external agents, including referral partners and third-party individuals, to assist in various aspects of student admissions and course enrolment. These external agents may be involved in collecting and processing personal data on behalf of the College.

13.2 Data Collection by External Agents

External agents, acting as independent entities, may collect student data on behalf of London Professional College during the admission and enrolment process. This may include personal and contact information, academic records, proof of identification, and other relevant details.

13.3 Security Measures for External Agents

Security Standards:
London Professional College mandates that external agents adhere to the same high standards of data security outlined in Sections 6 and 7 of this GDPR policy. This includes the use of encrypted communication channels, secure data storage practices, and regular security audits.

Training and Awareness:
External agents are required to undergo training on data protection principles and GDPR compliance. This training ensures that agents understand their responsibilities in safeguarding personal data and maintaining the confidentiality and integrity of the information collected.

13.4 Commission-Based Referrals

In cases where external agents are compensated on a commission basis for successful student referrals, the processing of personal data for commission calculations is outlined in this section. It is ensured that data processing is fair, transparent, and in compliance with applicable data protection laws.

13.5 Monitoring and Oversight

Oversight Mechanisms:
London Professional College maintains mechanisms for monitoring and overseeing the activities of external agents. This may include periodic reviews, assessments of data processing practices, and ensuring ongoing compliance with GDPR and relevant data protection regulations.

Feedback Channels:
The College encourages the use of feedback channels for reporting any concerns or potential non-compliance issues related to the activities of external agents. Such feedback is valuable in maintaining the integrity of data processing practices.

14. Data Subject Rights

14.1 Recognition of Data Subject Rights

London Professional College acknowledges and respects the rights of individuals concerning their personal data. In accordance with the GDPR, this section outlines the procedures in place to facilitate and uphold the rights of data subjects.

14.2 Right to Access Personal Data

Access Requests:
Individuals have the right to request access to their personal data held by the College. The College has established clear procedures for handling such requests, ensuring that individuals can obtain information about the processing of their data.

Verification of Identity:
To safeguard against unauthorised access, the College has implemented identity verification measures when responding to access requests. This ensures that the personal data is disclosed only to the rightful owner.

14.3 Right to Rectification

In the event that individuals identify inaccuracies or incomplete information in their personal data, they have the right to request rectification. The College has established procedures to promptly correct any inaccuracies and update personal data as necessary.

14.4 Right to Erasure (Right to be Forgotten)

Individuals have the right to request the erasure of their personal data under certain circumstances. The College ensures that clear procedures are in place for handling such requests and that erasure is carried out in accordance with legal and regulatory requirements.

14.5 Right to Restriction of Processing

In situations where the accuracy of personal data is contested, or processing is deemed unlawful, individuals have the right to request the restriction of processing. The College has procedures in place to assess and implement such restrictions as required by law.

14.6 Right to Data Portability

To empower individuals in their control over personal data, the College facilitates the right to data portability. This allows individuals to request the transfer of their personal data to another organisation. Procedures are in place to handle such requests securely and efficiently.

14.7 Right to Object to Processing

Individuals have the right to object to the processing of their personal data in certain circumstances, such as direct marketing. The College respects these objections and has mechanisms in place to cease processing where required.

14.8 Automated Decision-Making and Profiling

In cases of automated decision-making, including profiling, the College ensures transparency in the processes involved. Individuals are informed of the logic, significance, and potential consequences of such automated decisions.

14.9 Communication of Data Subject Rights

The College is committed to transparently communicating data subject rights to individuals. This includes providing clear information about how to exercise these rights, the procedures involved, and the expected timelines for response.

14.10 Data Protection Officer (DPO) Oversight

The Data Protection Officer (DPO) oversees the handling of data subject rights requests. The DPO serves as a point of contact for individuals seeking to exercise their rights and ensures that requests are processed in compliance with GDPR requirements.

14.11 Continuous Review and Improvement

The College actively encourages feedback from individuals regarding the exercise of their data subject rights. This feedback is invaluable in continuously reviewing and improving procedures to enhance the efficiency and effectiveness of the process.

By recognising and facilitating data subject rights, London Professional College aims to empower individuals to have greater control over their personal data. The College is committed to fostering a culture of transparency, accountability, and responsiveness in the handling of data subject rights requests.

15. Data Protection Officer (DPO) Contact Information

London Professional College designates a Data Protection Officer (DPO) responsible for overseeing data protection activities. The contact details of the DPO, including a dedicated email address and contact number, are provided for individuals to reach out with inquiries or concerns.

16. Cooperation with the ICO and Regulatory Authorities

The College commits to collaborating with the Information Commissioner's Office (ICO) and other regulatory authorities in matters related to data protection. This includes providing information requested by the ICO during investigations.

17. Employee and Agent Compliance

17.1 Training for Employees and Agents

All employees and external agents receive regular training on data protection principles, GDPR compliance, and their roles and responsibilities in safeguarding personal data.

17.2 Confidentiality Obligations

Employees and external agents are bound by confidentiality obligations regarding the processing of personal data. Breaches of confidentiality may result in disciplinary action.

By incorporating these additional sections into its GDPR policy, London Professional College ensures a comprehensive and legally compliant framework for the processing of personal data. This policy reflects the College's commitment to transparency, accountability, and the protection of individuals' privacy rights in accordance with UK data protection laws.

End of General Data Protection Regulation (GDPR) Policy

Version 1.23 | 30 Oct 2023

Contact Information

For inquiries or concerns regarding this GDPR policy, please contact:

Data Protection Officer (DPO):
[Name of DPO]
[Title of DPO]
[Email Address]
[Contact Number]

London Professional College
First Floor, Moorfoot House
221 Meridian Pl, Marsh Wall
London E14 9FJ

Phone: +44 (0) 20 3621 2479
Email: info@londonpc.org.uk
Web: www.londonpc.org.uk

Revision History

Version	Date	Changes Made	Author
1.23	30 Oct 2023	Initial creation of the policy	

This marks the conclusion of the GDPR policy for London Professional College. The document is subject to periodic review and updates to ensure continuous compliance with data protection regulations and alignment with the college's data processing practices.