POLICY
FOR PROCESSING PERSONAL DATA

COLEGIO
COLOMBO
BRITÁNICO

We Unite Peoples and Cultures
Through Education

Code PL-01 Version 01 **Last Review Date:** 2023-09-25	**POLICIES FOR PROCESSING PERSONAL DATA**

COLEGIO COLOMBO BRITÁNICO

We Unite Peoples and Cultures Through Education

1. LEGAL GROUNDS & APPLICATION

The policy for data processing is included in articles 15 and 20 of the Political Constitution, as well as in articles 17 item k) and 18 item f) of Statutory Law 1581, issued in 2012, according to which general provisions are set for the protection of personal data (LEPD). Additionally, article 2.2.2.25.1.1 section 1 chapter 25 of Decree 1074, issued in 2015, regulates partially Law 1581, issued in 2012.

This policy shall apply to all personal data recorded in data bases that are subject to processing by the person Responsible for Data Processing.

1.1 Scope

This document shall apply to all personal data or any other type of information used or filed in the data bases and files of CORPORACION COLEGIO COLOMBO BRITANICO, respecting the criteria for obtaining, collecting, using, processing, exchanging, transferring, and transmitting personal data, and setting obligations and guidelines of CORPORACION COLEGIO COLOMBO BRITANICO for managing and processing personal data filed in its data bases and files. This Manual applies to CORPORACION COLEGIO COLOMBO BRITANICO processes that must process data (public data, semi-private data, private data, sensitive data, data of chilren and adolescents) as Person Responsible for it and In Charge.

1.2 Applicable Regulations

- Political Constitution of Colombia
- Law 1581, issued in 2012
- Decree 1074, issued in 2015 Chapter 25 & Chapter 26 and:
  - Decree 1377, issued in 2013
  - Decree 886, issued in 2014
- Law 1266, issued in 2008 “Which sets general Habeas Data dispositions”.
- Administrative actions issued by the Superintendence of Industry and Commerce.

2. DEFINITIONS

The following definitions are set in article 3 of the LEPD and article 2.2.2.25.1.3 section 1 Chapter 25, Decree 1074, issued in 2015 (Article 3,Decree 1377, issued in 2013).

2.1. Authorization:

Previous, express, informed consent by Holder to process personal data.

2.2. Data Bases:

Set of personal data subject to being processed, belonging to a same context and stored systematically for future use.

2.3. Personal Data:

Any information linked or that may be linked to one or several designated or specifiable natural persons. This data is classified into public, semi-private, private and sensitive:

2.3.1. Public Data:

Data that is not semi-private, private, or sensitive. Public data, among others, include data related to the marital status of a person, his/her profession or occupation, business person or public employee. Due to its nature, public data may be included in public records, public documents, official magazines or publications, legal judgements duly executed that are not subject to privacy.

2.3.2. Semi-private Data:

Data that is not intimate, is not reserved data, nor public data, and whose disclosure may interest not only its Holder but certain sector or group of people or society in general such as: data bases containing financial, loans, credit, business service information that comes from third countries.

2.3.3. Private Data:

Personal data that, due to its intimate or reserved nature concerns only its Holder, and that in order to be processed requires its previous, express and informed authorization. Data bases containing telephone numbers, personal emails, work data, administrative or criminal violations data managed by tax entities, financial organizations and social security organizations, data bases on solvency or credit, data bases with enough information to analyze Holder's personality, data bases of person responsible for any operators rendering electronic communication services.

2.3.4. Sensitive Data:

Data that may affect Holder's intimacy or which improper use may result in discrimination, such as data disclosing race or ethnic origin, political orientation, religious or philosophical beliefs, belonging to unions, social organizations, human rights, or that promote the interests of any political party or that support the rights and guarantees of political parties that are the opposition parties, as well as data regarding health, sexual life and biometric data.

2.4. Person In Charge of Data Processing:

Natural or Legal Person, public or private, that by itself or associated with others, processes personal data on behalf of the Person Responsible for data processing.

2.5. Person Responsible for Data Processing:

Natural or Legal Person, public or private, by itself or associated with others, that makes decisions on data bases and/or data base processing.

2.6. Person Responsible for managing data bases:

Helper in charge of controlling and coordinating proper application of the policies for data processing already stored in a specific data base, as well as applying the guidelines set by the Person Responsible for data processing and the Data Protection Officer.

2.7. Data Protection Officer:

Natural person who assumes the duty to coordinate and implement the legal structure for protecting personal data. This person shall process Holders' requests for the exercise of the rights stated in Law 1581, issued in 2012.

2.8. Holder:

Natural Person whose personal data is subject to being processed.

2.9. Processing:

Any operation or series of operations on personal data such as collection, storage, use, circulation or removal.

2.10. Notification of Privacy:

Verbal or written communication made by the Person Responsible addressed to Holder for processing its personal data, according to which Holder is notified about the existence of policies for data processing that will be applied, the way to have access to such policies, and the purposes of data processing intended for the personal data.

2.11. Transfer:

Data transfer occurs when the Responsible person and/or Person In Charge of personal data processing in Colombia sends information or personal data to a receptor who, in turn, is responsible for the data processing and is located either in the country or out of the country.

2.12. Transmission:

Personal Data Processing that involves communication thereof within the territory of the Republic of Colombia or out of it when its purpose is to process such data on behalf of the responsible person.

3. PRINCIPLES OF DATA PROTECTION

Article 4 of LEPD states that for personal data processing to be performed in a harmonic and integral way according to the Law, the legal principles on data protection are as follows:

3.1. Rule of Law:

Data processing is an activity regulated by the LEPD, Decree 1377, issued in 2013, Chapter 25, Decree 1074, issued in 2015 and all other related provisions.

3.2. Principle of Purpose:

Data processing must have a true purpose according to the Constitution and the Law, which must be notified to Holder.

3.3. Principle of Freedom:

Data processing may only be done with the previous express informed consent by Holder. Personal data may not be obtained or disclosed without previous authorization, or, in case of absence of legal mandate that reveals consent. Data processing requires previous authorization by Holder by any means that allows Holder to be asked subsequently.

3.4. Principle of Accuracy or Quality: information being processed must be true, complete, accurate, updated, proven and understandable. Partial or incomplete data processing leading to error is forbidden.

3.5. Principle of Transparency:

The person responsible for or in charge of data processing must guarantee Data Holder the right to obtain, at any moment and without any restrictions, information about the existence of the concern data.

When requesting authorization from Holder, the responsible for data processing must notify in a clear and explicit way the following, keeping a proof that this requirement was duly met:

- Processing that will be used on the data and purpose thereof.
- Capacity of Holder's answer to questions made when these questions include sensitive data or data of children or adolescents.
- Rights as Holder.
- Identification, address, Email and telephone number of person responsible for data processing

3.6. Principle of Restricted Access and Circulation:

Data Processing is subject to limits derived from the nature of personal data, provisions of LEPD and the Constitution. In this sense, processing may only be made by authorized people or by the Holder and/or people as provided by the Law. Personal data, except for public information, may not be available on internet or other advertising channels or mass media, except if access is technically controllable to give restricted knowledge only to Holders or third parties duly authorized according to the Law.

3.7. Safety Principle:

Information processed by the Person Responsible or in Charge of Data Processing must be managed with the required technical, human, administrative measures required to grant legal certainty to the records and avoid unauthorized or fraudulent alteration, loss, consultation, use or access. The person responsible for data processing shall respond for implementing the corresponding safety measures and inform all personnel having direct or indirect access to data about these measures.

Users accessing the systems of information of the person responsible for data processing must know and meet all safety standards and measures corresponding to their duties. These safety standards and measures are set in the Internal Safety Policies PL-02 that must be followed by all users and company personnel. Any modification to the standards and measures regarding safety in personal data processing by the person responsible for data processing must be notified to the users.

3.8. Principle of Confidentiality:

All people involved in personal data processing that is not public are obliged to guarantee confidentiality of the information, even after its relationship with some of the duties that include data processing has ended. Thus, only provision or communication of personal data may be made when it applies to implementing the activities authorized by the LEPD and the terms thereof.

4. AUTHORIZATION FOR USE OF PERSONAL DATA

According to article 9 of LEPD, Holder's authorization is required for personal data processing, except in cases expressly indicated in the standards regulating protection of personal data. Previously and/or at the moment of collecting personal data, CORPORACION COLEGIO COLOMBO BRITANICO shall request Holder of personal data its authorization to collect and process such data, indicating the purpose for requesting such data, using automated technical means, either written or verbal, that allow them to keep a proof of such authorization and/or the contents of
article 2.2.2.25.2.2. section 2, Chapter 25, Decree 1074, issued in 2015.

Holder's authorization shall not be required when:

- Information is required by a public or administrative entity exercising its legal duties or by court/legal order.
- Information is public data.
- Cases of medical public health emergency.
- Data processing authorized by law for historical, statistical, or scientific purposes.
- Data related to the Civil Registry of people.

5. REQUEST AUTHORIZATION TO HOLDER OF PERSONAL DATA

Authorization for data use and/or processing shall be managed by CORPORACION COLEGIO COLOMBO BRITANICO with mechanisms that shall allow subsequent consultation and Holder's declaration as follows:

- In writing
- Orally.
- Through automated mechanisms.
- Through clear actions by Holder that allow to conclude in a reasonable way that Holder did grant its authorization.

CORPORACION COLEGIO COLOMBO BRITANICO, prior to and/or at the moment of collecting the personal data, shall notify Holder clearly the following:

a. The processing Holder's personal data will go through and the purpose thereof;
b. The optional or required character of the questions being asked, when these questions are about sensitive data or data of children and adolescents.
c. Rights as Holder;
d. Identification, physical address, email, telephone number of CORPORACION COLEGIO COLOMBO BRITANICO.

6. PERSON RESPONSIBLE FOR DATA PROCESSING

The person responsible for data processing in this policy is CORPORACION COLEGIO COLOMBO BRITANICO, and the contact data is:

- Address: AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA
- Email: habeasdata@ccbcali.edu.co
- Telephone: 5555385 - 6025555313

7. DATA BASES PROCESSING AND PURPOSES

CORPORACION COLEGIO COLOMBO BRITANICO, in accomplishing its business activity, processes personal data related to natural persons that are part of and are processed in data bases with authentic purposes, according to the Constitution and the law.
Personal data processing includes collection, storage, use, circulation, or removal. Data processing is subject to purposes authorized by Holder, as well as to the contractual obligations of the contracting parties, and where legal obligations must be met.
Attachment 1 PL-01 called Data Bases Organization includes information related to the various data bases which the company is responsible for, and the purposes assigned to each one of them for processing them.

8. EFFECTIVE PERIOD OF DATA BASES

Personal data included in the Data Bases shall be in effect during the period required to meet the purposes for which authorization is granted and the special standards regulating this subject.
Standards in effect related to the period of conservation shall also be taken into account.

9. HOLDERS' RIGHTS

According to article 8 of LEPD, article 2.2.2.25.4.1 section 4 Chapter 25, Decree 1074 issued in 2015 (Articles 21 & 22 Decree 1377, issued in 2013), Holders of data may exercise a series of rights regarding personal data processing.

a. know , update, and correct their personal data with the Person Responsible for Data Processing or Person In Charge of Data Processing. This right may be exercised with partial, inaccurate, incomplete, fractioned data that mislead to error, or those which data processing is expressly prohibited or has not been authorized;
b. Request proof of authorization granted to the Person responsible for data processing, except when it is expressly exempted as a requirement for data processing according to article 10 of this Law;
c. Be notified by the Person responsible for data processing or the person in charge of data processing, upon request, about the use it has given to Holder's personal data;
d. File any claims for violations before the Superintendence of Industry and Commerce according to this Law, and all other standards that may modify it, add it or complement it;
e. Revoke authorization and/or request removal of data when data processing does not respect the constitutional and legal principles, rights and guarantees. Revoking and/or removing shall proceed when the Superintendence of Industry and Commerce has determined that when processing data, the person responsible or in charge has participated in actions that are contrary to the law and the constitution;

f. Access at no cost, its personal data that has been subject to data processing.

The following rights may be exercised by these persons:

1. Holder, who shall prove its identity in full according to the means that the person responsible shall give Holder.
2. Persons entitled, whom shall prove such capacity.
3. Holder's representative and/or Proxy, upon filing proof of such power or representation.
4. By express stipulation on behalf of a third party or for a third party.

The rights of children and adolescents shall be exercised for people who are authorized to represent them.

9.1. Right to Data Access or Consultation

Holder's right to be notified by the person responsible for data processing, upon request, about the origin, use and purpose given to Holder's personal data.

9.2. Rights to Complaints and Claims

The Law states four types of claims:

- Claim of Correction: Holder right to update, correct, or modify partially, inaccurate, incomplete, fractioned, misleading data, or data which data process is expressly prohibited or has not been authorized.
- Claim of Withdrawal: Holder's right to withdraw data that is inappropriate, excessive, or that do not respect the Constitutional and legal principles, rights, and guarantees
- Revoking Claim: Holder's right to invalidate authorization previously granted for processing personal data
- Violation Claim: Holder's right to request remedy for not complying with the standards regarding Data Protection.

9.3. Right to request proof of authorization granted to the Person responsible for data processing

Except if expressly exempted as a requirement for data processing according to article 10 of LEPD.

9.4. Right to file claims for violations before the Superintendence of Industry and Commerce

Holder or entitled person shall only file a claim before the SIC – Superintendence of Industry and Commerce after consultation or claim before the person responsible for or in charge of data processing have failed.

10. PROCESSING UNDERAGE DATA

CORPORACION COLEGIO COLOMBO BRITANICO, according to article 7°, Law 1581, issued in 2012, processes children and adolescents' personal data as indicated in article 2.2.2.25.2.9 section 2, Chapter 25, Decree 1074, issued in 2015 (Article 12, Decree 1377, issued in 2013), under the following parameters and requirements:

1. that the use of data responds and respects the best interest of children and adolescents.
2. that in using data, the fundamental rights of minors are assured

Upon meeting the above requirements, CORPORACION COLEGIO COLOMBO BRITANICO shall request authorization to the legal representative of the children or adolescent, upon giving the minor/underage the chance to exercise its right to be listened to. Its opinion shall be analyzed considering its maturity, autonomy and capacity to understand the subject matter. As person responsible and/or in charge of the minor interests, it shall supervise the proper use of children's and adolescents' data by applying principles and obligations according to Law 1581, issued in 2012 and the corresponding regulations. Likewise, sensitive data collected or stored shall be identified with the purpose of increasing safety of data processing.

11. DUTIES AS PERSON RESPONSIBLE FOR DATA PROCESSING

CORPORACION COLEGIO COLOMBO BRITANICO, as person responsible for data processing shall meet the following duties without prejudice of all other provisions of this Law and others ruling its activity:

11.1. Regarding Holder:

a. Guarantee Holder, at all times, full and effective exercise of its right to habeas data;
b. Request and keep, according to this Law, a copy of the authorization granted by Holder
c. Properly notify Holder about the purpose of collecting data and the rights it has by virtue of the authorization granted
d. Process queries and claims according to the terms indicated in this Law;
e. Notify, by request of Holder, about the use given to its data;

11.2. Regarding the Person In charge:

a. Guarantee that the information provided to the Person In Charge of Data processing is true, complete, accurate, updated, verifiable and understandable.
b. Update information by notifying the Person In Charge in a timely way about all the updates on the data that was previously provided and follow all measures required so that the provided information is updated;
c. Correct the information if it is incorrect and notify the Person in Charge of data processing about it.
d. Notify the Person In Charge of data processing when certain information is under discussion by the Holder upon filing the claim and the corresponding formality has not been completed.
e. Provide the Person In Charge of Data Processing, if it applies, only data duly authorized to be processed according to the Law;
f. Demand the from the Person In Charge of Data Processing, at all times, respect for the safety and privacy conditions of Holder's information;

11.3. Regarding principles and other obligations:

a. Follow Rules of Law, principles of purpose, freedom, quality, accuracy, transparency, restricted accesss and circulation, safety and confidentiality.
b. Apply an internal manual of policies and procedures required to guarantee proper compliance of this Law, and, specially, for assistance in processing queries and claims.
c. Notify the data protection authority when there are any violations to the safety codes and there are risks involved in managing Holders' information.
d. Follow and meet all instructions and requirements demanded by the Superintendence of Industry and Commerce.
e. Keep information under the required safety conditions to avoid adulteration, loss, consultation, use or unauthorized or fraudulent access.

12. DUTIES AS PERSON IN CHARGE OF DATA PROCESSING

CORPORACION COLEGIO COLOMBO BRITANICO, as person in Charge of Data Processing shall perform the following duties, without prejudice of all other dispositions of this Law and others ruling its activity:

a. Guarantee Holder, at all times, full and effective exercise of habeas data right;
b. Keep information under the required safety conditions to avoid adulteration, loss, consultation, use or unauthorized or fraudulent access;
c. Make timely updates, corrections or removal of data, according to this Law;
d. Update information reported by the Responsible of Data Processing within the 5 working days after its reception;
e. Process queries and claims filed by Holders according to the terms herein indicated;

f. Follow a manual of internal policies and procedures to assure proper compliance of this Law, and, particularly, for answering queries and claims by Holders;
g. Insert the notice “Claim in process” in the form regulated in this Law;
h. Insert the notice “information under dispute”, after being notified by the competent authorities about legal processes related to the quality of personal data;
i. Refrain from disseminating information that is being disputed by Holder and has been blocked by the Superintendence of Industry and Commerce;
j. Allow access to information only to people authorized to access it
k. Notify the Superintendence of Industry and Commerce when there are violations to the safety codes and when there are risks in managing Holders’ information.
l. Follow instructions and meet requirements as set by the Superintendence of Industry and Commerce.

13. ASSISTANCE TO DATA HOLDERS

In order to respond to requirements, queries and claims regarding personal data protection, CORPORACION COLEGIO COLOMBO BRITANICO has designated a Data Protection Officer. Data Holders may file their requests or queries or consults through the following channels:
Email: habeasdata@ccbcali.edu.co
Address: AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA.
Telephones: 5555385 - 6025555313

14. PROCEDURES TO EXERCISE HOLDERS’ RIGHTS

14.1. Right to Data Access or Consultation

CORPORACION COLEGIO COLOMBO BRITANICO shall guarantee holder’s consult free from any charges in the following cases: (Article 2.2.2.25.4.2. section 4 Chapter 25, Decree 1074, issued in 2015):

1. At least once every calendar month.
2. Every time there are significant modifications to the policies for data processing that encourage new consults

For consults that are more frequent than one calendar month, CORPORACION COLEGIO COLOMBO BRITANICO may charge Holder for expenses such as delivery, reproduction, and, in this case, certification of documents. Costs of reproduction (copies) may not exceed costs of recovering the corresponding material. To that end CORPORACION COLEGIO COLOMBO BRITANICO shall

evidence before the Superintendence of Industry and Commerce, whenever required, such expenses.

Data Holder may exercise its right to access or right to consult its data with a written request addressed to CORPORACION COLEGIO COLOMBO BRITANICO, duly sent by email to: habeasdata@ccbcali.edu.co, indicating the subject: “Exercise the right to access or right to consult data”, or by postal mail to this address: AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA. The request must include the following data: :

- Holder’s name and surnames.
- Copy of Holder’s Citizenship Card, and, if required, the person who is acting on its behalf, as well as the document certifying this. .
- Request where access or consult are stated.
- Address for notifications, date and signature of requester.
- Documents supporting the request when applicable.

Holder may choose from the following ways of consulting the data bases to receive the requested information:

- Screen display.
- In writing with copy or photocopy sent by certified mail or not.
- Email, or other electronic mean.
- Another system that is appropriate for the configuration of the data bases or the nature of data processing offered by CORPORACION COLEGIO COLOMBO BRITANICO.

After receiving the request, CORPORACION COLEGIO COLOMBO BRITANICO shall solve the request for consulting in a period of ten (10) working days from the date of reception thereof. In case it is not possible to solve a request for consultation within such period of time, the concern shall be informed indicating the reasons for such delay and indicating the date its consult shall be solved. In any event, it may exceed five working days following expiration of the first period. These terms are set in article 14 of the LEPD.

Once the consultation process has finished, Holder or its successor may file a claim before the Superintendence of Industry and Commerce.

14.2. Rights to Complaints and Claims

Data Holder may exercise its rights to complain and make claims about its data in writing addressed to CORPORACION COLEGIO COLOMBO BRITANICO sent by email to habeasdata@ccbcali.edu.co, indicating the subject matter “Exercise of the right to access or right to consult”, or by postal mail addressed to AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA. The request shall include the following data::

- Holder's name and surnames.
- Copy of the Citizenship Card of Holder, and if required, the person who represents it, as well as the document supporting such representation.
- Description of the facts and request indicating correction, elimination, suppression, revoking or inflation.
- Address for notifications, date and signature of requester.
- Documents supporting the request filed that may want to validate when necessary.

If the claim is incomplete, the concern shall be asked to remedy this within a period of maximum (15) fifteen days following reception of the claim. After two (2) months from the date of the request, without requester filing the required information, it will be understood that requester has desisted from the claim.

Upon receiving the full claim, the notice "claim in process" shall be inserted in the data base, as well as the reason for it, in a period no greater than two (2) working days. Such notice shall stay until the claim is remedied.

CORPORACION COLEGIO COLOMBO BRITANICO shall solve the petition for claim in a period of maximum 15 days following the date of reception thereof. If it is not posible to solve the claim within such term, the concern shall be informed of the reasons for the delay and the date in which such claim will be processed which, in any event, may not exceed eight (8) working days following expiration of the first term.
Upon completion of the claim process, Holder or its successor may file a claim before the Superintendence of Industry and Commerce.

14.3. People authorized to receive information

CORPORACION COLEGIO COLOMBO BRITANICO shall provide information of Holders from its data bases to the following authorized people, according to article 13, Law 1581, issued in 2012:

- Holders, its successors or legal representatives;
- Public or Administrative Organizations exercising their legal duties or court order.
- Third parties authorized by Holder or by Law.

14.3.1. Verification of authorization to request or receive information

For processing a request for claim or consult, requester shall provide the following documents to prove that it is the Holder or is authorized to receive the requested information, as follows:

- Holder: Copy of Identification Document.
- Successor: Identification Document, civil registry of death of Holder, document supporting capacity to act as such, and copy of the identification document of Holder.
- Legal representative and/or proxy: valid identification document, document that supports its capacity (power of attorney) and copy of identification document of Holder.

15. DATA PROCESSING IN VIDEO-SURVEILLANCE SYSTEMS

CORPORACION COLEGIO COLOMBO BRITANICO shall inform people about the existence of video-surveillance equipment by posting visible signs that all Holders may see and installing them in areas of video-surveillance, mainly in areas of entrance into the places that are being surveilled and monitored inside these places.

These signs shall include who is responsible for data processing, purposes of data processing, Holder rights, channels available for exercising Holder rights, as well as where is the policy for data processing placed and published.

On the other hand, images will be stored only for the time strictly required to meet the purpose, and it will file the database where images are stored in the National Registry of Data Bases, except if processing is only the reproduction or emission of images live.

Access and dissemination of images shall be restricted to people authorized by Holder and/or by request of an authority that is exercising its duties. Consequently, dissemination of information collected shall be controlled and consistent with the purpose set by the Person Responsible for Data Processing.

16. SAFETY MEASURES

CORPORACION COLEGIO COLOMBO BRITANICO, in meeting the safety principle according to article 4 item g) of the LEPD, has implemented technical, human and administrative measures required to guarantee safety of all records avoiding fraud, loss, consultation, unauthorized use, or access, and implementing technical, human and administrative measures required to guarantee safety of the records and avoiding adulteration, loss and unauthorized or misleading, consult, use or access.

On the other hand, CORPORACION COLEGIO COLOMBO BRITANICO, has held transmission contracts, has required people in charge of data processing to work in the implementation of the safety measures necessary to guarantee safety and confidentiality of the information in personal data processing.

Safety measures implemented by CORPORACION COLEGIO COLOMBO BRITANICO included in PL-02 Internal Safety Policies (Tables I, II, III & IV) are as follows:

TABLE I: Common Safety Measures for all kinds of data (public, private, confidential, reserved) and data bases (automated, not automated)	
Documents & Support	1. Measures that prevent inappropriate Access or recover of data that has been discarded, erased, or destructed. 2. Restricted Access to a place where data is stored. 3. Authorization by the responsible person to manage data bases for taking out documents or support documents either physically or electronically. 4. Labeling or identification system for type of information. 5. Inventory of supporting documents
Access control	1. Limited access of users to data required for the performance of its duties. 2. Updated list of authorized users and access. 3. Mechanisms to avoid access to data with other permissions different from the authorized ones 4. Granting, alteration, cancellation of permissions by authorized personnel.
Incidents	1. Recording incidents: type of incident, time when it occurred, who made the notification, effects and correcting measures. 2. Notification procedure and management of incidents
Personnel	1. Definition of duties and obligations of users with data access. 2. Definition of control duties and authorizations assigned by the person responsible for data processing. 3. Dissemination of standards among personnel and consequences of breach thereof.
Internal Safety Manual	1. Preparation and implementation of the Manual for mandatory compliance by personnel. 2. Minimum contents: application scope, measures, safety procedures, duties, obligations, description of data bases, incidents procedure, identification of people in charge of data processing.

TABLE II: Common Safety Measures for all kinds of data (public, private, confidential, reserved) depending on the type of data base	
Non Automated Data Bases	
File	Filing documents following procedures that guarantee correct conservation, localization and consultation that allow Holders to exercise their rights.
Storage of documents	Storage devices with mechanisms that prevent access of unauthorized people
Custody of documents	Duty of care and custody ty the person in charge of documents during data review or processing
Automated Data Bases	

Identification and authentication	Personalized Identification of users to gain access to information and verification systems of its authorization. Identification and authentication mechanisms; passwords: allocation and expiration date.
Telecommunications	Access to data through safe networks

TABLE III: Safety measures for private data depending on the type of data bases	
Non-automated Data Bases	
Audit	1. Ordinary audits (internal or external) every two months. 2. Extraordinary audits due to significant modifications in the systems of information. 3. Deficiency detection report and corrections proposal 4. Analysis and conclusions by the person responsible for safety and for data processing
Responsible for safety	1. Appointment of one or several administrators of data bases. 2. Appointment of one or several people in charge of control and coordination of measures for the Internal Safety Manual 3. Prohibition of delegation of responsibility for managing data base administrators.
Internal Safety Manual	1. Regular compliance controls
Automated Data Bases	
Documents & support documents management	1. Record incoming and outgoing documents, support documents: date, issuer, receptor, number, type of information, information delivery method, person responsible for handing in and receiving.
Access control	1. Access control into the place or places where the systems of information are located.
Identification y authenticatcion	1. Mechanism to limit the number of failed attempts to unauthorized access. 2. Mechanisms for encrypting data to be transmitted.
Incidents	1. Record procedures for data recovery, the person who does it, restore data, and data saved manually. 2. Authorization by the person responsible for processing recovery procedures

TABLE IV: Safety Measures for sensitive data, depending on the type of Data Bases	
Non-automated Data Bases	
Access Control	1. Access exclusively for authorized personnel. 2. Mechanism of access identification. 3. Record unauthorized users access. 4. Destruction of things that prevent access or data recovery.
Documents storage	1. Filing cabinets, office cabinets or similar furniture located in access areas protected with keys or other locks. 2. Measures to prevent manipulation of documents stored physically.
Automated Data Bases	
Access control	1. System of confidential labeling.

Identification & authentication	1. Encrypting mechanisms for transmission and storage
Documents storage	1. Record access: user, time, data base being accessed, type of access, record being accessed 2. Control record of access by person responsible of safety. Monthly report
Telecommunications	1. Access & transmission of data through safe electronic networks. 2. Data transmission using encrypted networks (VPN).

17. COOKIES OR WEB BUGS

CORPORACION COLEGIO COLOMBO BRITANICO may collect personal information from its users while using the Webpage, the Application or the Landing Page. Users may store this personal information on the webpage, the application or the landing page with the purpose of facilitating transactions and services to be rendered by CORPORACION COLEGIO COLOMBO BRITANICO and/or its landing page. Therefore, CORPORACION COLEGIO COLOMBO BRITANICO uses various follow-up and data collection technologies such as Cookies belonging to CCB as well as to third parties. This analysis tool helps owners of the webpage and applications understand how visitors interact with its properties. This tool may be used with all cookies to gather information and offer statistics of use of webpages without identifying personally Google visitors.

This information allows us to know surfing patterns and offer personalized services. CORPORACION COLEGIO COLOMBO BRITANICO may use these technologies for authentication to remember preferences in using the webpage, the application, and the Landing Page, to make offers that may be of interest, and to facilitate transactions, to analyze use of webpage, application or landing pages and their services, to use it or combine it with personal information that we have and share it with authorized organizations.

If a user does not want its personal information to be collected through Cookies, it may change preferences in its own browser. Notwithstanding, it is important to indicate that, if a browser does not accept Cookies, some of the webpage, the application or Landing Page functions with may not be available or work correctly.

Blocking or eliminating Cookies installed in the device may be allowed by configuring the options on the browser installed in your device, as follows:

- **Chrome:** https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=es
- **Microsoft Edge:** https://support.microsoft.com/es-es/microsoft-edge/permitir-temporalmente-las-cookies-y-los-datos-del-sitio-en-microsoft-edge-597f04f2-c0ce-f08c-7c2b-541086362bd2
- **Firefox:** https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-web-rastrear-preferencias
- **Safari:** https://support.apple.com/es-es/HT201265

18. NOTIFICATION, MANAGEMENT AND RESPONSE PROCEDURES IN CASE OF INCIDENTS/ISSUES

CORPORACIÓN COLEGIO COLOMBO BRITÁNICO has an incident reporting procedure for communication and notification among collaborators, personal data protection officers, data processors, data owners, inspection and control government entities, as well as judicial branch authorities: for the management and response to security incidents from the moment they are detected in order to make an evaluation and manage the vulnerabilities identified, ensuring that systems, networks and applications are sufficiently secure.

All users and those responsible for managing databases, as well as any person involved in the collection, storage, use, circulation or any processing or consultation of the school databases, must know the procedure to act in case of security incidents to ensure the confidentiality, availability and integrity of the information contained in the databases under their responsibility.

Some examples of security incidents are: failure of security systems that allow access to personal data to unauthorized persons, unauthorized attempt to exit a document or medium, loss of data or total or partial destruction of media, change of physical location of databases, knowledge of passwords by third parties, modification of data by unauthorized personnel, among others.

In the event of a security incident, the response team or committee shall take into account the following criteria:

Strategy to identify, contain and mitigate security incidents.

- Implement measures to contain and reverse the impact of the security incident.
- Adequately assess the security incident and its impact on the data subjects.
- Verify the legal or contractual requirements with service providers associated with the security incident.
- Determine the level of risk to information holders and report the occurrence.
- Verify the roles and responsibilities of the personnel responsible for the operation of the affected information or data.
- Timeline for security incident management.
- Apply the procedure for dealing with security incidents, according to parameters that allow an adequate management and mitigation of impact. Verify, according to the evaluation of the security incident, the need to notify entities such as: the Attorney General's Office, , Gaula, National Police, The Financial Superintendence of Colombia, Police Cybernetic Center, colCERT; Police CSIRT, Asobancaria, CSIRT, Sector CSIRT, among others.

Progress of the security incident report

Monitor the management by establishing deadlines, evaluate its progress and identify possible conflicting points that may arise in the handling of the security incident.

Security incident response evaluation

Once the security incident has been managed and controlled, the response team should review the actions taken to contain it and make the appropriate adjustments to implement the improvement plan.

Actions implemented and improvement plans.

Establish the necessary actions to mitigate the impact of the security incident and prevent its recurrence, through corrective and preventive actions, as well as improvement plans to be adopted by the response team.

Documentation and reporting to the oversight and control entity.

Document in an internal record the information related to the security incident, as well as prepare a report with support of the actions taken, which must be filed with the Superintendence of Industry and Commerce, through the RNBD within 15 working days after the incident has been detected.

Review.

Evaluation of the causes that led to the security incident and the success of its management to assess the effectiveness of the controls and actions implemented. Document lessons learned to be taken into account on future occasions.

19. MANAGING RISKS RELATED TO DATA PROCESSING

CORPORACION COLEGIO COLOMBO BRITANICO has identified risks related to personal data processing and it has set controls with the purpose of mitigating its causes by implementing PL-02 Internal Safety Policies. Therefore, it shall set a risk management system and tools, indicators, and required resources for its management whenever the organizational structure, the processes and internal procedures, the quantity of data bases and types of personal data processed by the organization are considered at risk or exposed to frequent high-impact situations that affect the service rendered or attempt against Holders information.

The risk-management system shall determine the sources such as: technology, human resource, infrastructure and processes that require protection, their vulnerabilities and threats, with the purpose

of assessing the risk level. Thus, in order to guarantee personal data protection, it shall consider the type or group of internal/external people, the various levels of access authorizations. Likewise, the probability of occurrence of any type of event or action that may produce damage (material or immaterial) shall also be observed. Such as:

- Criminality: understood as actions caused by humans who violate the Law and that are penalized by the Law.
- Events with physical origin: understood as natural and technical events, as well as events indirectly caused by human intervention.
- Institutional Negligence and decisions: understood as actions, decisions or omissions by people who have the power or influence over the system. At the same time, they are the less predictable threats, as they are directly related to the human behavior.

CORPORACION COLEGIO COLOMBO BRITANICO shall implement protection measures in the risk management program to avoid or minimize the damage in case a threat is realized.

20. HANDING IN PERSONAL DATA TO AUTHORITIES

Whenever a public or administrative entity in the exercise of its legal powers or by court order requests COLEGIO COLOMBO BRITANICO access and/or release of personal data included in its Data Bases, legality of the request shall be requested, as well as belonging of requested data with regards to the purpose expressed by the authority. When handing in the data, a minute shall be issued indicating the data of the requesting entity and the characteristics of the personal information requested, indicating the obligation to guarantee Holder's rights from the officer making the request as well as from the person receiving it and the requesting authority.

21. INTERNATIONAL TRANSFER and TRANSMISSION OF PERSONAL DATA

CORPORACION COLEGIO COLOMBO BRITANICO shall transfer personal data to countries that provide proper levels of data protection. A country offering proper levels of data protection is a country that meets the standards set by the Superintendence of Industry and Commerce about the subject, which in no event may be lower than those that Law 1581, issued in 2012 demands its recipients. This prohibition shall not rule when it is about:

- Information which Holder has granted its express and clear authorization to be transferred.
- Exchange of medical data, when Holder's data processing is mandatory for public health and hygiene.

- Bank or financial transfers, according to international treaties where the Republic of Colombia is a part of, based on the principle of reciprocity.
- Transfers required for the execution of a contract between Holder and the person responsible for data processing, or for compliance with pre-contractual measures; provided that Holder's authorization is granted.
- Transfers legally demanded for safeguarding public interest, exercising or defending a right to a legal proceeding.

In cases where transfer of data is required and the destination country is not in the list of countries considered safe ports as indicated by the Superintendence of Industry and Commerce, a declaration of relative conformity regarding the international transfer of personal data shall be processed before the Superintendence.

International transfers made by CORPORACION COLEGIO COLOMBO BRITANICO and a person in charge to allow that the person in charge may process data on behalf of the person responsible, shall not require notification to the Holder or obtain Holder's consent, provided that there is a contract for personal data transmission. This contract for transmission of personal data shall be subscribed between the Responsible person and the Person in Charge to define the scope of personal data processing under their control and responsibility, as well as the activities that the person in charge shall perform on the Responsible person's account and the obligations that the person in Charge shall meet for Holder. Additionally, the person in Charge shall meet the following obligations and apply the standards in effect in Colombia regarding data protection.

1. Process personal data, on behalf of the Responsible person according to principles ruling them
2. Protect Data Bases containing personal data and keep it safe.
3. Keep the confidentiality of personal data

The above conditions set for international data transmissions shall also apply to national data transmission.

22. PROCESSING BIOMETRIC DATA

Biometric data stored in Data Bases are exclusively collected for safety reasons to check personal identity and control access of employees, clients, and visitors. Biometric mechanisms of identification capture, process and store information related to, among others, physical features of the people (fingerprints, voice recognition and facial aspects), in order to establish or "authenticate" the identity of each individual.

Management of Biometric Data Bases is done under the technical safety measures that guarantee proper compliance with the principles and obligations derived from the Statutory Law in Data Protection, assuring confidentiality and secrecy of Holders' information.

23. NATIONAL REGISTRY OF DATA BASES – RNBD

The term for registering Data Bases on the RNBD shall be legally established. Likewise, according to article 12, issued in 2014, the persons responsible for data processing shall register their Data Bases in the National Registry of Data Bases on the data that Superintendence of Industry and Commerce indicates for such registration, according to instructions given by that organization. The Data Bases created after this term, must be registered within the 2 following months from the date of its creation.

24. SAFETY OF INFORMATION AND PERSONAL DATA

Compliance of the regulations under the Personal Data Protection framework, safety, confidentiality and or secrecy of information stored in Data Bases is of vital importance for CORPORACION COLEGIO COLOMBO BRITANICO. Thus, we have set information safety policies, guidelines, and procedures that may change at any time adapting to new ways and needs of CORPORACION COLEGIO COLOMBO BRITANICO, considering that its goal is to protect and preserve the integrity, confidentiality and availability of information and personal data.

Likewise, we assure that in collecting, storing, using and/or processing, destructing, or eliminating information provided, we rely on technological safety tools and implement safety practices that include: transmission and storage of sensitive information through safe mechanisms, use of safe protocols, assuring technological components, restricting access to information only to authorized personnel, making backups, using safe software development, among others.

In case it is necessary to provide information to a third party, due to the existence of a contractual bond, we subscribe a transmission contract to assure information secrecy and confidentiality, as well as compliance of this Data Processing Policy, manuals of information safety and protocols for assisting Holders as set by CORPORACION COLEGIO COLOMBO BRITANICO. In any event, we follow commitments of protection, care, safety, and preservations of confidentiality, integrity and privacy of stored data.

25. PROCESSING DOCUMENTS

Documents including personal data must be easily recoverable. Thus, the location where each document either hardcopy or virtual, is stored must be documented. Frequent inspections to these

routes must be made. Conservation of this data must be performed, considering the environmental conditions, places for storage, risks data faces, and others. Time for keeping the documents shall be determined considering legal requirements if they apply, or else, each organization shall set it according to its needs. Likewise, Final disposition of the documents shall be clear, identifying if it's going to be recycled, reused, kept, or digitized, among others.

Documents related to personal data protection must be prepared by personnel or other competent organization. Likewise, the organization must be the inspecting person checking and approving all documents and record this information in the space for document approval.

In order to make them easily traceable, the documents shall be codified, updated and modified by the persons responsible. This modification shall be made if it is necessary. For elimination purposes, it must be justified as described in the historic file that is located in the lower part of all documents.
Documents that are hardcopies or digital including personal data must be protected by external or internal agents that may alter its contents according to PL-02 Internal Manual of Safety Policies.

Distribution of documents including personal data will be made by the person responsible for data processing. It will document the evidence of such distribution, where it will specify: type of document and identification of the recipient person.
A person responsible for guaranteeing confidentiality of Holders' personal data shall be appointed. This person will be in charge of having custody over the documents, guarantee their protection, hardcopy as well as digital, avoid information alteration. Likewise, it will guarantee that the documents taken out of custody are duly identified and easily traceable.

26. EFFECTIVE PERIOD

This update of the Policy will be in effect from 2023-09-25. Data Bases that are the responsibility of CORPORACION COLEGIO COLOMBO BRITANICO shall be subject to data processing during the reasonable and necessary time required for the purpose for which data was collected and according to authorization granted by Holders of Personal Data.

27. ANNEXES

Does not apply

28.DOCUMENT PREPARATION AND APPROVAL

REVISIÓN Y APROBACIÓN DEL DOCUMENTO

Prepared by:	PROTECDATA COLOMBIA S.A.S	**Approved by :**	
		Position:	
Date :	2023-09-25	**Date:**	

29.HISTORICAL REPORT OF DOCUMENTS

DATE	VERSION	DESCRIPTION OF CHANGE
2023-09-11	01	General legal and technical document update.