POLICY
FOR PROCESSING PERSONAL DATA

COLEGIO
COLOMBO
BRITÁNICO

We Unite Peoples and Cultures
Through Education

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

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

CORPORACION COLEGIO COLOMBO BRITANICO sets a procedure for notifying, managing, and responding to incidents with the purpose of guaranteeing confidentiality, availability and integrity of information included in the Data Bases that it is responsible for.

Users and person responsible for the procedures, as well as any person related to storage, management or consult of Data Bases included in this document, must know the procedure to act in case of incidents.

The procedure for notification, management and response of incidents is as follows:

- When a person comes into knowledge of an incident (loss, theft and/or unauthorized access) affecting or that may affect the confidentiality, availability and integrity of the protected information of the company or any of the people in charge, that person must notify it immediately to the Data Protection Officer, uncovering in detail the type of incident, the people that might have been related to it, the date and time of the incident, the person notifying the incident, the person who is taking the notification and the effects produced.
- Upon notifying the incident, the Data Protection Officer must be asked for a certificate of reception where notification of incident is evidenced as well as all of the above requirements.
- CORPORACION COLEGIO COLOMBO BRITANICO, creates a record of incidents (internal or external fraud, damages to physical assets, technological failure, execution and management of processes), date and time thereof, person notifying incident, effects of incidents and correcting measures when it applies. This record is processed by the Data Protection Officer, and forwarded to FR-08 Record of Safety Incidents.
- Likewise, procedures must be implemented to recover data when it applies, indicating who performs the process, restored data, and, if applicable, the data required to be saved manually in the recovery process.
- Additionally, the Data Protection Officer must notify the Superintendence of Industry and Commerce, through an RNBD within a period of 15 working days following detection thereof.
- Finally, CORPORACION COLEGIO COLOMBO BRITANICO shall notify Holders about the incident when it is fully identified that Holders may be significantly affected.

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.

POLÍTICA
DE TRATAMIENTO
DE DATOS PERSONALES

COLEGIO
COLOMBO
BRITÁNICO

We Unite Peoples and Cultures
Through Education

Código PL-01	**POLÍTICAS DE TRATAMIENTOS DE DATOS PERSONALES**
Versión 01	
Fecha de última revisión: 2023-09-25	

GENTES MORESQUE DOCENDO IUNGIMUS

COLEGIO COLOMBO BRITÁNICO

We Unite Peoples and Cultures Through Education

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN

La política de tratamiento de la información se desarrolla en cumplimiento de los artículos 15 y 20 de la Constitución Política, así como, con fundamento en los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD). Adicionalmente, en cumplimiento del artículo 2.2.2.25.1.1 sección 1 capítulo 25 del Decreto 1074 de 2015, por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el Responsable del tratamiento.

1.1 Alcance

El presente documento aplicará para todos aquellos datos personales o de cualquier otro tipo de información que sea utilizada o repose en las bases de datos y archivos de CORPORACION COLEGIO COLOMBO BRITANICO, respetando los criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, y fijar las obligaciones y lineamientos de CORPORACION COLEGIO COLOMBO BRITANICO para la administración y tratamiento de los datos personales que reposen en sus bases de datos y archivos. El presente Manual es aplicable a los procesos de CORPORACION COLEGIO COLOMBO BRITANICO que deban realizar el Tratamiento de los datos (datos públicos, datos semiprivados, datos privados, datos sensibles, datos de los niños, niñas y adolescentes), en calidad de Responsable y de Encargado.

1.2 Normatividad Aplicable

- Constitución Política de Colombia
- Ley 1581 de 2012
- Decreto 1074 de 2015 Capítulo 25 y Capítulo 26 compilatorios de los decretos:
  - Decreto 1377 de 2013
  - Decreto 886 de 2014
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data”.
- Actos administrativos expedidos por la Superintendencia de Industria y Comercio.

2. DEFINICIONES

Las siguientes definiciones se encuentran establecidas en el artículo 3 de la LEPD y artículo 2.2.2.25.1.3 sección 1 Capítulo 25 del decreto 1074 de 2015 (Artículo 3 del decreto 1377 de 2013).

2.1 Autorización:

Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

2.2 Base de datos:

Conjunto organizado de datos personales que sea objeto de tratamiento, pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

2.3 Dato personal:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Estos datos se clasifican en públicos, semiprivados, privados y sensibles:

2.3.1. Dato público:

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o del servidor público.
Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

2.3.2. Dato semiprivado:

Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

2.3.3. Dato privado:

Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

2.3.4. Dato sensible:

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

2.4. Encargado del tratamiento:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Responsable del tratamiento.

2.5. Responsable del tratamiento:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

2.6. Responsable de administrar las bases de datos:

Colaborador encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base datos específica; así como de poner en práctica las directrices que dicte el Responsable del tratamiento y el Oficial de Protección de datos.

2.7. Oficial de protección de Datos:

Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012.

2.8. Titular:

Persona natural cuyos datos personales sean objeto de tratamiento.

2.9. Tratamiento:

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

2.10. Aviso de privacidad:

Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

2.11. Transferencia:

La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del tratamiento y se encuentra dentro o fuera del país.

2.12. Transmisión:

Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento determinado por el encargado por cuenta del responsable.

3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

El artículo 4 de la LEPD establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

3.1. Principio de Legalidad:

El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD, el Decreto 1377 de 2013 Compilado en el Capítulo 25 del Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

3.2. Principio de Finalidad:

El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

3.3. Principio de Libertad:

El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad.

3.4. Principio de Veracidad o Calidad:

La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

3.5. Principio de transparencia:

En el tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del tratamiento o del Encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como Titular.
- La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

3.6. Principio de Acceso y Circulación Restringida:

El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la LEPD y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

3.7. Principio de Seguridad:

La información sujeta a tratamiento por el Responsable del tratamiento o Encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El Responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento de todo el personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del Responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el PL-02 Políticas Internas de Seguridad, de obligado cumplimiento para todo usuario y personal de la empresa. Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

3.8. Principio de Confidencialidad:

Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de la misma.

4. AUTORIZACIÓN USO DE DATOS PERSONALES

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización del Titular, salvo en los casos expresamente señalados en las normas que reglamentan la protección de los datos personales. Con antelación y/o al momento de efectuar la recolección del dato

personal, CORPORACION COLEGIO COLOMBO BRITANICO solicitará al Titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015.

No será necesaria la autorización del Titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

5. SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL

La autorización para el uso y/o tratamiento de los datos será gestionada por CORPORACION COLEGIO COLOMBO BRITANICO, a través de mecanismos que garanticen su consulta posterior y la manifestación de la voluntad del Titular a través de los siguientes medios:

- Por escrito.
- De forma oral.
- Mediante canales automatizados.
- Mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización.

CORPORACION COLEGIO COLOMBO BRITANICO, con antelación y/o al momento de efectuar la recolección del dato personal, informará de manera clara y expresa al Titular, lo siguiente:

a. El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
b. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
c. Los derechos que le asisten como Titular;
d. La identificación, dirección física o electrónica y teléfono CORPORACIÓN COLEGIO COLOMBO BRITÁNICO.

6. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es CORPORACION COLEGIO COLOMBO BRITANICO, cuyos datos de contacto son los siguientes:

- Dirección: AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA
- Correo electrónico: habeasdata@ccbcali.edu.co
- Teléfono: 5555385 - 6025555313

7. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

CORPORACION COLEGIO COLOMBO BRITANICO, en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley. El tratamiento al cual serán sometidos los datos personales incluye recolección, almacenamiento, uso, circulación o supresión. El tratamiento de los datos estará sujeto a las finalidades autorizadas por el Titular, a las obligaciones contractuales entre las partes, así como, a los casos en los cuales existan obligaciones legales que deba cumplir.
El Anexo 1 PL-01 denominado Organización Bases de Datos, contiene la información relativa a las distintas bases de datos responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento.

8. VIGENCIA DE LA BASE DE DATOS

Los datos personales incorporados en las bases de datos estarán vigentes durante el plazo necesario para cumplir las finalidades para el cual se autorizó su tratamiento y de las normas especiales que regulen la materia, también se tendrán en cuenta las normas vigentes relacionadas con el periodo de conservación.

9. DERECHOS DE LOS TITULARES

De acuerdo con el artículo 8 de la LEPD, artículo 2.2.2.25.4.1 sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículos 21 y 22 del Decreto 1377 de 2013), los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. El Titular de los datos personales tendrá los siguientes derechos:

a. Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;

b. Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;
c. Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;
d. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
e. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución;
f. Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Estos derechos podrán ejercerse por las siguientes personas.

1. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el Responsable.
2. Por sus causahabientes, quienes deberán acreditar tal calidad.
3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
4. Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos

9.1 Derecho de acceso o consulta

Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

9.2 Derechos de quejas y reclamos

La Ley distingue cuatro tipos de reclamos:

- Reclamo de corrección: el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

- Reclamo de supresión: el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
- Reclamo de revocación: el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- Reclamo de infracción: el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

9.3. Derecho a solicitar prueba de la autorización otorgada al Responsable del tratamiento

Salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.

9.4. Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones

El Titular o causahabiente solo podrá elevar ante la SIC – Superintendencia de Industria y Comercio la petición (queja), una vez haya agotado el trámite de consulta o reclamo ante el Responsable del tratamiento o Encargado del tratamiento.

10. TRATAMIENTO DE DATOS DE MENORES

CORPORACION COLEGIO COLOMBO BRITANICO de acuerdo con el artículo 7° de la Ley 1581 de 2012, realiza Tratamiento de datos personales de niños, niñas y adolescentes en el marco de los criterios señalados en el artículo 2.2.2.25.2.9 sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 12 del Decreto 1377 de 2013), con observancia de los siguientes parámetros y requisitos:

1. Que el uso del dato responda y respete el interés superior de los niños, niñas y adolescentes.
2. Que en el uso del dato se asegure el respeto de sus derechos fundamentales del menor.

Cumplidos los anteriores requisitos, CORPORACION COLEGIO COLOMBO BRITANICO solicitará al representante legal del niño, niña o adolescente la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. En calidad de Responsable y/o Encargado velará por el uso adecuado de los datos de niños, niñas y adolescentes aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y normas reglamentarias. Asimismo, identificará los datos sensibles recolectados o almacenados con el fin de incrementar la seguridad y tratamiento de la información.

11. DEBERES COMO RESPONSABLE DEL TRATAMIENTO

CORPORACION COLEGIO COLOMBO BRITANICO en calidad de Responsable del Tratamiento cumplirá los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

11.1. Frente al Titular:

a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b. Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
c. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
d. Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;
e. Informar a solicitud del Titular sobre el uso dado a sus datos;

11.2. Frente al Encargado:

a. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
b. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
c. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
d. Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
e. Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;
f. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

11.3. Frente a los principios y otras obligaciones:

a. Observar los principios Legalidad, finalidad, libertad, calidad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad
b. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;
c. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

d. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
e. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

12. DEBERES COMO ENCARGADO DEL TRATAMIENTO

CORPORACION COLEGIO COLOMBO BRITANICO en calidad de Encargado del Tratamiento cumplirá los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
c. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;
d. Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
e. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;
f. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;
g. Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley;
h. Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
i. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
j. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
k. Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
l. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

13. ATENCIÓN A LOS TITULARES DE DATOS

Para la atención de peticiones, consultas y reclamos en materia de protección de datos personales, CORPORACION COLEGIO COLOMBO BRITANICO ha designado un Oficial de protección de datos. Los Titulares de los datos podrán remitir sus peticiones o consultas a través de los siguientes canales:
Correo electrónico: habeasdata@ccbcali.edu.co
Dirección: AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA.
Teléfonos: 5555385 - 6025555313

14. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

14.1. Derecho de acceso o consulta

CORPORACION COLEGIO COLOMBO BRITANICO garantizará al Titular la consulta de forma gratuita de sus datos personales en los siguientes casos (Artículo 2.2.2.25.4.2. sección 4 capítulo 25 del Decreto 1074 de 2015):

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, CORPORACION COLEGIO COLOMBO BRITANICO podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, CORPORACION COLEGIO COLOMBO BRITANICO demostrará a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a CORPORACION COLEGIO COLOMBO BRITANICO enviado, mediante correo electrónico a: habeasdata@ccbcali.edu.co, indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación. – Petición en que se concreta la solicitud de acceso o consulta. – Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por CORPORACION COLEGIO COLOMBO BRITANICO.

Una vez recibida la solicitud, CORPORACION COLEGIO COLOMBO BRITANICO resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

14.2. Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a CORPORACION COLEGIO COLOMBO BRITANICO enviado, mediante correo electrónico a habeasdata@ccbcali.edu.co, indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a AV LA MARIA PANCE 69, CALI - VALLE DEL CAUCA. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

CORPORACION COLEGIO COLOMBO BRITANICO resolverá la petición de reclamo en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.
Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

14.3. Facultados para recibir información

CORPORACION COLEGIO COLOMBO BRITANICO suministrará la información de los Titulares de sus bases de datos a las siguientes personas habilitadas o facultadas para recibirla, de acuerdo con el artículo 13 de la Ley 1581 de 2012:

- A los Titulares, sus causahabientes o sus representantes legales;
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
- A los terceros autorizados por el Titular o por la ley.

14.3.1. Verificación de la facultad para solicitar o recibir información

Para la gestión de la solicitud de consulta o reclamo, el solicitante deberá aportar los siguientes documentos para acreditar su titularidad o la facultad para recibir la información requerida, de acuerdo con los siguientes casos:

- Titular: Copia del documento de identidad.
- Causahabiente: Documento de identidad, registro civil de defunción del Titular, documento que acredite la calidad en que actúa y copia del documento de identidad del Titular.
- Representante legal y/o apoderado: Documento de identidad válido, documento que acredite la calidad en la que actúa (Poder) y copia del documento de identidad del Titular.

15. TRATAMIENTO DE DATOS EN LOS SISTEMAS DE VIDEOVIGILANCIA

CORPORACION COLEGIO COLOMBO BRITANICO informará a las personas sobre la existencia de mecanismos de videovigilancia, mediante la fijación de anuncios visibles al alcance de todos los titulares e instalados en las zonas de videovigilancia, principalmente en las zonas de ingreso a los

lugares que están siendo vigilados y monitoreados y al interior de estos. En estos avisos informará quién es el Responsable del Tratamiento, las finalidades del tratamiento, los derechos del Titular, los canales habilitados para ejercer los derechos del Titular, así como, dónde se encuentra publicada la Política de Tratamiento de la Información.
De otra parte, conservará las imágenes solo por el tiempo estrictamente necesario para cumplir con la finalidad del e inscribirá la base de datos que almacena las imágenes en el Registro Nacional de Bases de Datos, salvo que el Tratamiento consista solo en la reproducción o emisión de imágenes en tiempo real.
El acceso y divulgación de las imágenes será restringido a personas autorizadas por el Titular y/o por solicitud de una autoridad en ejercicio de sus funciones. En consecuencia, la divulgación de la información que se recolecta será controlada y consistente con la ¬finalidad establecida por el Responsable del Tratamiento.

16. MEDIDAS DE SEGURIDAD

CORPORACION COLEGIO COLOMBO BRITANICO, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, CORPORACION COLEGIO COLOMBO BRITANICO, mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por CORPORACION COLEGIO COLOMBO BRITANICO que están recogidas y desarrolladas en su PL-02 Políticas Internas de Seguridad (Tablas I, II, III y IV).

TABLA I: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) y bases de datos (automatizadas, no automatizadas)	
Gestión de documentos y soportes	Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. Acceso restringido al lugar donde se almacenan los datos. Autorización del responsable de Administrar las bases de datos para la salida de documentos o soportes por medio físico o electrónico. Sistema de etiquetado o identificación del tipo de información. Inventario de soportes.

Control de acceso	Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. Lista actualizada de usuarios y accesos autorizados. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. Concesión, alteración o anulación de permisos por el personal autorizado
Incidencias	Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. Procedimiento de notificación y gestión de incidencias.
Personal	Definición de las funciones y obligaciones de los usuarios con acceso a los datos. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.
Manual Interno de Seguridad	Elaboración e implementación del Manual de obligado cumplimiento para el personal. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento.

TABLA II: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) según el tipo de bases de datos	
Bases de datos no automatizadas	
Archivo	Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta, que permitan el ejercicio de los derechos de los Titulares.
Almacenamiento de documentos	Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.
Custodia de documentos	Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.
Bases de datos automatizadas	
Identificación y autenticación	Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. Mecanismos de identificación y autenticación; Contraseñas: asignación y caducidad.
Telecomunicaciones	Acceso a datos mediante redes seguras.

TABLA III: Medidas de seguridad para datos privados según el tipo de bases de datos	
Bases de datos no automatizadas	
Auditoría	Auditoría ordinaria (interna o externa) cada dos meses. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. Informe de detección de deficiencias y propuesta de correcciones. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
Responsable de seguridad	Designación de uno o varios Administradores de las bases de datos. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. Prohibición de delegación de la responsabilidad del Responsable del tratamiento en los Administradores de las bases de datos.
Manual Interno de Seguridad	Controles periódicos de cumplimiento.
Bases de datos automatizadas	
Gestión de documentos y soportes	Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.
Control de acceso	Control de acceso al lugar o lugares donde se ubican los sistemas de información.
Identificación y autenticación	Mecanismo que limite el número de intentos reiterados de acceso no autorizados. Mecanismos de cifrado de datos para la transmisión.
Incidencias	Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA IV: Medidas de seguridad para datos sensibles según el tipo de bases de datos	
Bases de datos no automatizadas	
Control de acceso	Acceso solo para personal autorizado. Mecanismo de identificación de acceso. Registro de accesos de usuarios no autorizados. Destrucción que impida el acceso o recuperación de los datos.
Almacenamiento de documentos	Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas. Medidas que impidan el acceso o manipulación de documentos almacenados de forma física.
Bases de datos automatizadas	
Control de acceso	Sistema de etiquetado confidencial.
Identificación y autenticación	Mecanismos de cifrado de datos para la transmisión y almacenamiento.
Almacenamiento de documentos	Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede Control del registro de accesos por el responsable de seguridad. Informe mensual.
Telecomunicaciones	Acceso y transmisión de datos mediante redes electrónicas seguras. Transmisión de datos mediante redes cifrados (VPN).

17. COOKIES O WEB BUGS

CORPORACION COLEGIO COLOMBO BRITANICO puede recolectar información personal de sus Usuarios mientras utilizan la Página Web, la Aplicación o las Páginas Vinculadas (Landing Page). Los usuarios pueden optar por almacenar esta información personal en la página web, la aplicación o en el portal vinculado (Landing Page), con el fin de facilitar las transacciones y los servicios a prestar por parte del CORPORACION COLEGIO COLOMBO BRITANICO y/o de sus portales vinculados (Landing Page). Por lo que, CORPORACION COLEGIO COLOMBO BRITANICO utiliza diferentes tecnologías de seguimiento y recopilación de datos como, Cookies propias y de terceros, esta es la herramienta de análisis que ayuda a los propietarios de sitios web y de aplicaciones a entender cómo interactúan los visitantes con sus propiedades. Esta herramienta puede utilizar un conjunto de cookies para recopilar

información y ofrecer estadísticas de uso de los sitios web sin identificar personalmente a los visitantes de Google.
Esta información nos permite conocer sus patrones de navegación y ofrecerle servicios personalizados. CORPORACION COLEGIO COLOMBO BRITANICO podrá utilizar estas tecnologías para autenticarlo, para recordar sus preferencias para el uso de la página web, la aplicación y las páginas vinculadas (Landing Page), para presentar ofertas que puedan ser de su interés y para facilitar transacciones, para analizar el uso de la página web, la aplicación o de las páginas vinculadas y sus servicios, para usarla en el agregado o combinarla con la información personal que tengamos y compartirla con las entidades autorizadas.
Si un usuario no quiere que su información personal sea recogida a través de Cookies, puede cambiar las preferencias en su propio navegador web. No obstante, es importante señalar que, si un navegador web no acepta Cookies, algunas de las funcionalidades de la página web, la aplicación y/o las páginas vinculadas (Landing Page) podrían no estar disponibles o no funcionar correctamente. Puede permitir, bloquear o eliminar las cookies instaladas en su dispositivo mediante la configuración de las opciones del navegador instalado en su dispositivo, así:

- **Chrome:** https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=es
- **Microsoft Edge:** https://support.microsoft.com/es-es/microsoft-edge/permitirtemporalmente-las-cookies-y-los-datos-del-sitio-en-microsoft-edge-597f04f2-c0ce-f08c7c2b-541086362bd2
- **Firefox:** https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-webrastrear-preferencias
- **Safari:** https://support.apple.com/es-es/HT201265

18. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

CORPORACION COLEGIO COLOMBO BRITANICO establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

- Cuando una persona tenga conocimiento de una incidencia (perdida, hurto y/o acceso no autorizado) que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa o alguno de los Encargados deberá comunicarlo, de manera inmediata, al Oficial de Protección de Datos, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.
- Una vez comunicada la incidencia ha de solicitar al Oficial de Protección de Datos un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.
- CORPORACION COLEGIO COLOMBO BRITANICO, crea un registro de incidencias que debe contener: el tipo de incidencia (Fraude Interno o externo, Daños a activos físicos, Fallas tecnológicas, Ejecución y administración de procesos), fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el Oficial de Protección de Datos, remitirse al FR-08 Registro de incidentes de seguridad.
- Asimismo, debe implementar los procedimientos para la recuperación de los datos cuando aplica, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.
- Adicional, el Oficial de Protección de Datos debe informar a la Superintendencia de Industria y Comercio, mediante el RNBD dentro de los 15 días hábiles siguientes de haber sido detectado.
- Finalmente, CORPORACION COLEGIO COLOMBO BRITANICO notificará del incidente a los Titulares, cuando se identifique que puedan verse afectados de manera significativa.

19. ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS

CORPORACION COLEGIO COLOMBO BRITANICO ha identificado riesgos relacionados con el tratamiento de los datos personales y establecidos controles con el fin de mitigar sus causas, mediante la implementación de la PL-02 Políticas Internas de Seguridad. Por ello, establecerá un sistema de gestión de riesgos junto con las herramientas, indicadores y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de base datos y tipos de datos personales tratados por la organización se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra la información de los titulares.

El sistema de gestión de riesgos determinará las fuentes tales como: tecnología, recurso humano, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo. Por lo que, para garantizar la protección de datos personales se tendrá en

cuenta el tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), tales como:

- Criminalidad: Entendida como las acciones, causadas por la intervención humana, que violan la ley y que están penalizadas por ésta.
- Sucesos de origen físico: Entendidos como los eventos naturales y técnicos, así como, los eventos indirectamente causados por la intervención humana.
- Negligencia y decisiones institucionales: Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

CORPORACION COLEGIO COLOMBO BRITANICO en el programa de gestión de riesgo implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

20. ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES

Cuando por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial se soliciten a CORPORACION COLEGIO COLOMBO BRITANICO acceso y/o entrega de datos de carácter personal contenidos en cualquiera de sus bases de datos, se verificará la legalidad de la petición, la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad. Para la entrega se suscribirá un acta indicando los datos de la entidad solicitante y las características de la información personal solicitada, precisando la obligación de garantizar los derechos del Titular, tanto al funcionario que hace la solicitud, a quien la recibe, así como a la entidad requirente.

21. TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES

CORPORACION COLEGIO COLOMBO BRITANICO realizará transferencia de datos personales a países que proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la Ley 1581 de 2012 exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.

- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos en los cuales sea necesaria la transferencia de los datos y el país de destino no se encuentre en el listado de países considerados como puertos seguros señalados por la Superintendencia de Industria y Comercio, se deberá gestionar ante el mismo ente una declaración de conformidad relativa a la aprobación para la transferencia internacional de datos personales.

Las transmisiones internacionales de datos personales que se efectúen entre CORPORACION COLEGIO COLOMBO BRITANICO y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales. Este contrato de transmisión de datos personales deberá suscribirse entre el Responsable y el Encargado para definir el alcance del tratamiento de datos personales bajo su control y responsabilidad, así como, las actividades que el encargado realizará por cuenta del Responsable y las obligaciones del Encargado para con el titular. Adicionalmente, el Encargado deberá cumplir con las siguientes obligaciones y aplicar las normas vigentes en Colombia en materia de protección de datos.

1. Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
3. Guardar confidencialidad respecto del tratamiento de los datos personales.

Las anteriores condiciones fijadas para las transmisiones de datos internacionales, también le serán aplicables a las transmisiones de datos nacionales.

22. TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos almacenados en las bases de datos son recolectados y tratados por motivos estrictamente de seguridad, para verificar la identidad personal y realizar control de acceso a los empleados, clientes y visitantes. Los mecanismos biométricos de identificación capturan, procesan y almacenan información relacionada con, entre otros, los rasgos físicos de las personas (las huellas dactilares, reconocimiento de voz y los aspectos faciales), para poder establecer o “autenticar” la identidad de cada sujeto.

La administración de las bases de datos biométrica se ejecuta con medidas de seguridad técnicas que garantizan el debido cumplimiento de los principios y las obligaciones derivadas de Ley Estatutaria en Protección de Datos asegurando además la confidencialidad y reserva de la información de los titulares.

23. REGISTRO NACIONAL DE BASES DE DATOS – RNBD

El término para registrar las bases de datos en el RNBD será el establecido legalmente. Asimismo, de acuerdo con el artículo 12 del Decreto 886 de 2014, los Responsables del Tratamiento deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos en la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. Las bases de Datos que se creen con posterioridad a ese plazo deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

24. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

El cumplimiento del marco normativo en Protección de Datos Personales, la seguridad, reserva y/o confidencialidad de la información almacenada en las bases de datos es de vital importancia para CORPORACION COLEGIO COLOMBO BRITANICO. Por ello, hemos establecido políticas, lineamientos y procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento ajustándose a nuevas normas y necesidades de CORPORACION COLEGIO COLOMBO BRITANICO cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales.

Asimismo, garantizamos que en la recolección, almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

En caso de ser necesario suministrar información a un tercero por la existencia de un vínculo contractual, suscribimos contrato de transmisión para garantizar la reserva y confidencialidad de la información, así como, el cumplimiento de la presente Política del tratamiento de los datos, de las políticas y manuales de seguridad de la información y los protocolos de atención a los titulares establecidos en CORPORACION COLEGIO COLOMBO BRITANICO. En todo caso, adoptamos compromisos para la protección, cuidado, seguridad y preservación de la confidencialidad, integridad y privacidad de los datos almacenados.

25. GESTIÓN DE DOCUMENTOS

Los documentos que contengan datos personales deben ser fácilmente recuperables, es por ello que se debe dejar documentado el lugar donde reposa cada uno de los documentos tanto físicos como digitales, se deben hacer inspecciones a estas rutas de almacenamiento de forma frecuente, se debe garantizar su conservación dejando definido en que soporte y bajo qué condiciones se llevará a cabo esta conservación, teniendo en cuenta condiciones ambientales, lugares de almacenamiento, riesgos a los cuales están expuestos entre otros, el tiempo de retención de los documentos se determina en función de los requisitos legales si aplica, de lo contrario cada organización lo define de acuerdo a sus necesidades, así mismo debe tener clara la disposición final de los mismos, identificando si se recicla, reutiliza, se conserva, se digitaliza entre otros.

Los documentos que tienen que ver con la protección de datos personales deben ser elaborados por personal o una entidad competente para ello, así mismo la organización debe ser quien revise y apruebe todos los documentos y lo deje registrado en la casilla de aprobación de los documentos.

A finde que sean fácilmente trazables, los documentos deberán estar codificados, serán actualizados y modificados por el personal responsable, esta modificación se efectuara siempre y cuando sea necesario, para la eliminación de un documento se debe tener la justificación para ello descrita en el histórico el cual se encuentra en la parte inferior de todos los documentos.

Los documentos tanto físicos como digitales que contengan datos personales, deben ser protegidos por agentes externos o internos que puedan alterar su contenido, siguiendo los lineamientos descritos en el PL-02 Manual Interno de Políticas de Seguridad.

La distribución de los documentos que contengan datos personales la efectuara el responsable del tratamiento, este dejará documentada la evidencia de dicha distribución, donde entre otros se especifique; el tipo de documento y la identificación de la persona a la cual se le entregó la información

Se deberá designar un responsable de garantizar la confidencialidad de los datos personales de los titulares, este será quien custodie documentos, garantice su protección tanto física como digital, evite alteraciones de la información, así mismo garantizará que los documentos que salgan de su custodia sean identificados y fácilmente trazables.

26. VIGENCIA

La presente actualización de la Política estará vigente desde el 2023-09-25, las bases de datos responsabilidad de CORPORACION COLEGIO COLOMBO BRITANICO serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos y de acuerdo con la autorización otorgada por los Titulares de los datos personales.

27. APÉNDICE

No aplica

28. ELABORACIÓN Y APROBACIÓN DEL DOCUMENTO

REVISIÓN Y APROBACIÓN DEL DOCUMENTO			
Elaborado por:	PROTECDATA COLOMBIA S.A.S	**Aprobado por:**	
		Cargo:	
Fecha:	2023-09-25	**Fecha:**	

29. HISTÓRICO DE DOCUMENTOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
2023-09-11	01	Actualización jurídica y técnica general del documento.