



DATA PROCESSING POLICIES AND PROCEDURES INTERNAL HANDBOOK

POL-028-E

**COMPREHENSIVE
CULTURE OF EXCELLENCE**

**COMMITTED COMMUNITY
THE ENGLISH WAY**

**EFFECTIVE GOVERNANCE
AND FINANCIAL SUSTAINABILITY**

1. Legal Basis and Scope of Application	2
2. Definitions set out in Article 3 of the Data Protection Law and Chapter 25, Section 1, Article 2.2.2.25.1.3 of Decree 1074 of 2015.....	3
3. Principles of Data Protection	4
4. Authorisation of the processing policy	5
5. Processing and purpose of the databases	6
6. Special categories of data	7
6.1. Children and Adolescents' Rights	7
6.2. Sensitive data	8
7. Data Controller	9
8. Rights of the Data Subjects	9
9. Attention to Data Subjects	10
10. Functions and duties	10
10.1. Data Controller	10
10.2. Security Officers	11
10.3. Users	12
11. Procedures for exercising the Data Subject's rights.....	14
11.1. Right of access or consultation	14
11.2. Complaints and grievances rights	15
12. Infringements and penalties.....	16
13. Security measures	16
14. Navigation data	19
15. Cookies or web bugs.....	19
16. Transfer of data to third countries	20
17. Related policies.....	20
18. Approval and details for review	21
19. Validity	21
20. Version Control.....	21

1. Legal Basis and Scope of Application

The information processing policy is developed in compliance with Articles 15 and 20 of the Political Constitution; Articles 17 paragraph k) and 18 paragraph f) of the Statutory Law 1581 of 2012, by which general provisions are issued for the Protection of Personal Data (LEPD); and Chapter 25 Section 3 Article 2.2.2.2.25.3.2 of Decree 1074 of 2015, which partially regulates the previous Law.

This policy will be applicable to all personal data registered in databases that are processed by the Data Controller and is addressed to all data users, which are both own staff and external staff of the FUNDACIÓN EDUCATIVA DE INGLATERRA.

When the Data Subject gives his or her consent for the data to form part of a database of an institution, whether public or private, legal or natural, the latter becomes the Data Controller and acquires a series of obligations such as: (i) to treat such data with security and caution, (ii) to ensure its integrity and (iii) to appear as the body to which the Data Subject may address for the monitoring of the information and its control, being able to exercise his or her rights of consultation and claims.

Although the controller is responsible for the processing of data, his or her competences are embodied in the functions that correspond to his or her service staff. The staff of the institution responsible for the processing with direct or indirect access to databases containing personal data must be familiar with the data protection regulations and the data protection policies internal handbook of the Institution. They must, therefore, comply with the data security obligations corresponding to their functions and position.

To ensure compliance with its security obligations, the FUNDACIÓN EDUCATIVA DE INGLATERRA appoints four (4) security officers responsible for developing, coordinating, controlling and verifying compliance with the security measures mentioned in this handbook.

This policy shall apply to all personal data recorded in databases processed by the Data Controller and is addressed to all data users, which are both staff of the FUNDACIÓN EDUCATIVA DE INGLATERRA and external staff.

All users involved in the storage, processing, consultation or any other activity related to personal data and information systems are obliged to comply with the security measures established for the processing of data and are subject to the duty of confidentiality, even after the end of their employment or professional relationship with the organisation responsible for the processing.

Confidentiality, set out in Article 4 (h) of the Data Protection Law, is formalised through the signing of a confidentiality agreement between the user and the Data Controller.

2. Definitions set out in Article 3 of the Data Protection Law and Chapter 25, Section 1, Article 2.2.2.25.1.3 of Decree 1074 of 2015

- **Authorisation:** Prior, express and informed consent of the Data Subject to carry out the processing of personal data.
- **Database:** An organised set of personal data that is the subject of processing.
- **Personal Data:** Any information linked or capable of being linked to one or more specific or identifiable natural person(s).
- **Data Processor:** A natural or legal person, public or private, who, alone or in association with others, carries out the processing of personal data on behalf of the controller.
- **Data Controller:** Natural or legal person, public or private, who alone or in association with others, decides on the database and/or the processing of the data.
- **Data Subject:** Natural person whose personal data is the subject of processing.
- **Processing:** Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.
- **Privacy Notice:** Verbal or written communication generated by the Data Controller, addressed to the Data Subject for the processing of his/her personal data, by means of which the Data Subject is informed about the existence of the data processing policies that will be applicable, the way to access them and the purposes of the processing that is intended to be given to the personal data.
- **Public Data:** Data that is not semi-private, private or sensitive. Public data includes, among others, data relating to the civil status, their profession, and their status as traders or public servants. Due to their nature, public data may be contained, among others, in public registers, public documents, official gazettes and bulletins and duly enforced court rulings that are not subject to confidentiality.
- **Sensitive Data:** Sensitive data is understood to be that which affects the privacy of the Data Subject or whose improper use may lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical convictions, membership of labour unions, social organisations, human rights organisations or organisations that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sex life and biometric data.
- **Data Transfer:** The transfer of data takes place when the Data Controller and/or Data Processor of personal data, located in Colombia, sends the information or personal data to a recipient, which in turn is a Data controller and is located inside or outside the country.
- **Data Transmission:** Processing of personal data that involves the communication of such data within or outside the territory of the Republic of Colombia when the purpose of the processing is to be carried out by the Data Processor on behalf of the Data Controller.

3. Principles of Data Protection

Article 4 of the Data Protection Law establishes principles for the processing of personal data that must be applied harmoniously and comprehensively in the development, interpretation and application of the law. The legal principles of data protection are as follows:

- **Lawfulness:** The processing of data is a regulated activity that must be subject to the provisions of the Data Protection Law, Decree 1377 of 2013 and other provisions that develop it.
- **Purpose:** The processing must obey a legitimate purpose in accordance with the Constitution and the law, which must be informed to the Data Subject.
- **Freedom:** Processing may only be carried out with the prior, express and informed consent of the Data Subject. Personal data may not be obtained or disclosed without prior authorisation, or in the absence of a legal or judicial mandate revealing consent. The processing of data requires the prior and informed consent of the Data Subject by any means that allows for subsequent consultation, except in the following cases exempted by Article 10 of the Data Protection Law:
 - Information required by a public or administrative body in the exercise of its legal functions or by court order.
 - Data of a public nature.
 - Cases of medical or health emergencies.
 - Processing of information authorised by law for historical, statistical or scientific purposes.
 - Data related to the Civil Registry of persons.
- **Accuracy:** The information subject to processing must be truthful, complete, accurate, up-to-date, verifiable and comprehensible. The processing of partial, incomplete, fragmented or misleading data is prohibited.
- **Transparency:** The right of the Data Subject to obtain from the Data Controller or Data Processor, at any time and without restriction, information about the existence of data concerning him/her, must be guaranteed in the processing. At the time of requesting the Data Subject's authorisation, Data Controller must clearly and expressly inform him/her of the following, keeping proof of compliance with this duty:
 - The processing to which your data will be subjected and the purpose of such processing.
 - The optional nature of the Data Subject's response to the questions asked when these deal with sensitive data or data on children or adolescents.

- Your rights as Data Subject.
 - The identification, physical address, e-mail address and telephone number of the Data Controller.
- **Principle of Restricted Access and Circulation:** Processing is subject to the limits arising from the nature of the personal data, the provisions of the Data Protection Law and the Constitution. In this sense, the processing may only be carried out by persons authorised by the Data Subject and/or by the persons provided for in the law. Personal data, except for public information, may not be made available on the internet and other means of dissemination or mass communication, unless access is technically controllable to provide restricted knowledge only to Data Subjects or authorised third parties in accordance with the law.
 - **Security:** The information subject to processing by the Data Controller or Data Processor shall be handled with the technical, human and administrative measures necessary to ensure the security of the records, preventing their adulteration, loss, consultation, unauthorised or fraudulent use or access. The Data Controller is responsible for implementing the corresponding security measures and for informing all staff who have direct or indirect access to the data. Users accessing the Data Controller's information systems must be aware of and comply with the security rules and measures corresponding to their functions. These security rules and measures are set out in this handbook, which must be complied with by all users and staff of the FUNDACIÓN EDUCATIVA DE INGLATERRA. Any modification of the rules and measures regarding the security of personal data by the Data Controller must be brought to the attention of the users.
 - **Principle of Confidentiality:** All persons involved in the processing of personal data that are not of a public nature are obliged to guarantee the confidentiality of the information, even after the end of their relationship with any of the tasks involved in the processing, and may only supply or communicate personal data when this corresponds to the development of the activities authorised in the Data Protection Law and under the terms of the same.

4. Authorisation of the processing policy

In accordance with Article 9 of the Data Protection Law, the processing of personal data requires the prior and informed authorisation of the Data Subject. By accepting this policy, any Data Subject who provides information regarding their personal data is consenting to the processing of their data by the FUNDACIÓN EDUCATIVA DE INGLATERRA, under the terms and conditions set forth herein.

Authorisation from the Data Subject is not required in the case of:

- Information required by a public or administrative body in the exercise of its legal functions or by court order.
- Data of a public nature.
- Cases of medical or health emergencies.
- Processing of information authorised by law for historical, statistical or scientific purposes.
- Data related to the civil registration of persons.

5. Processing and purpose of the databases

The FUNDACIÓN EDUCATIVA DE INGLATERRA, in the course of its activities, processes personal data relating to natural persons that are contained and processed in databases for legitimate purposes, in compliance with the Constitution and the Law.

The following table (Table I) presents the different databases managed by the FUNDACIÓN EDUCATIVA DE INGLATERRA and the purposes assigned to each of them.

Table I. Databases and purposes

Name	Purpose
Staff (Active and Inactive)	The data will be used for the following purposes: Requesting data concerning personal identification, contact information, academic data, work, professional and financial history data, properly developing the process of registration and employment linkage or contracting for the provision of services; entrance and retirement examinations, occupational examinations, sending personalised content and detailed information on the functions of the position; implementing labour well-being actions; disseminate job offers to participate in internal staff selection processes at the Institution; communicate institutional information; carry out activities for statistical purposes; develop registration processes for congresses, events or seminars organised by the Institution; update data and verify the identity of employees, use biometric data for admission, use of the cafeteria and other managed systems; summoning applicants in the selection process to scheduled interviews, carrying out home visits, verifying work and personal references, work experience and professional career, supplying information to companies with which there is an agreement for the recruitment of foreign teachers or members of the management, and to the employees' fund, preparation of equipment items, sending information via text messages and e-mails, delivery and allocation of equipment to employees, drafting of Human Resources reports, process of affiliation to the social security system and compensation funds of employees and their beneficiaries, delivery of employment references, use of photographic images and videos for corporate purposes, obtaining and providing data on employees' children in the development of recreational and welfare activities through the Institutions or allied entities, performance evaluations, surveys, application of the psychosocial risk battery, generation of work certifications, promotions, transfers, retirement interviews, in internal and external auditing and control processes, in the delivery of mandatory institutional reports, deactivation of information systems, management of affiliation and withdrawal of employee and cooperative funds, reports of termination of employment contract and reporting thereof to the social security system, administrative processes before the Ministry of National Education, the UGPP, DIAN, and all those with purposes directly related to or derived from the Employment Contract, the above purposes are enunciative and not exhaustive.

<p>Parents and students</p> <p>(Admissions - enrolment and Health Care users)</p>	<p>The data will be processed in accordance with the following purposes: for purposes directly related to or derived from this Enrolment Contract, including the development of academic and extracurricular activities and the use of digital platforms, related to the educational process and the FOUNDATION.</p> <p>Consolidate the information of parents and students to have contact with them when required, send information, use of photographs, images and videos for the promotion of the establishments owned by the FUNDACIÓN EDUCATIVA DE INGLATERRA and its activities, use of biometric data for entrance, exit and cafeteria control, enrolment, information for official bodies (ICFES, MEN, SIRE, SED, DANE and ICBF, insurers, parent associations, etc.), FUNDACIÓN EDUCATIVA DE INGLATERRA, Use of biometric data for entrance, exit and cafeteria control, enrolment, information for official bodies (ICFES, MEN, SIRE, SED, DANE and ICBF), insurance companies, parents' associations linked to the FOUNDATION (and its educational establishments), other educational centres, registration of grades, evaluations and everything related to the educational development of the child.</p> <p>The data is recorded for the control and consultation of admission of the educational community, especially underage students, for records of sensitive medical history data (student data, health services, background information, informed consent, medical certificates) and medical formulation and reports to the Invita.</p> <p>Conduct interviews with the different groups in the institution (Psychologists, Head of Admissions, Directors of Section, teachers).</p> <p>Security studies, central risk consultations, monitoring reports for budget projection, income and withdrawal reports, entrance talks.</p> <p>Alumni data for sending information on events to be held at the Institution, job and study offers, consultations, surveys, use of images for the annual mosaics, sending of transcripts.</p>
<p>Providers</p>	<p>The data will be used for the following purposes: Request for bids and economic proposals for the acquisition of products and services; for the analysis and viability of each product and/or service; sending communications via text messages and emails; submission of relevant reports to the different control entities; review and verification of commercial references; pre-contractual and contractual negotiations; provision of information in internal and external auditing processes that are carried out within the institution; use of biometric data for the registration of income, use of photographic images or videos for institutional purposes, sending information on products, services or news of the foundation; tracking in restrictive databases such as (Police, Attorney General, Comptroller, SARLAFT - Risk Management System for Money Laundering and Financing of Terrorism and others that the Colombian regulations provide) the above purposes are illustrative and not exhaustive.</p>
<p>Biometric data</p> <p>(Parents and students - Staff - Providers and Visitors - Video surveillance)</p>	<p>The data will be used for the following purposes. Authorising entry to the different areas or departments of the institution; entry reports for students, teachers, administrative staff, providers, contractors and any individual wishing to enter the facilities. Sending information in text messages and e-mails for promotional and/or informative purposes; the above purposes are enunciative and not exhaustive.</p>

6. Special categories of data

6.1. Children and Adolescents' Rights

The processing of personal data of children and adolescents is prohibited, except in the case of data of a public nature, and when such processing complies with the following requirements:

- That it responds to and respects the best interests of children and

adolescents.

- To ensure that their fundamental rights are respected.

Once the above requirements have been met, the legal representative of the child or adolescent will grant authorisation after the minor has exercised his or her right to be heard, an opinion that will be assessed taking into account the maturity, autonomy and capacity to understand the matter.

It is the task of the State and educational bodies of all kinds to provide information and training to legal representatives and guardians about the possible risks faced by children and adolescents with regard to the improper processing of their personal data, and to provide knowledge about the responsible and safe use by children and adolescents of their personal data, their right to privacy and the protection of their personal information and that of others.

All persons responsible and in charge involved in the processing of personal data of children and adolescents shall ensure the proper use of such data, complying at all times with the principles and obligations set out in the Data Protection Law and Decree 1074 of 2015. In any case, the processing shall ensure respect for the prevailing rights of children and adolescents.

The rights of access, correction, suppression, revocation or claim for infringement of the data of children and adolescents will be exercised by the persons who are empowered to represent them.

6.2. Sensitive data

Sensitive data are those that affect the privacy of the Data Subject or whose improper use may lead to discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership of labour unions, social organisations, human rights organisations or those that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sex life and biometric data.

According to Article 6 of the Data Protection Law, the processing of sensitive data is prohibited, except when:

- The Data Subject has given his or her explicit consent to such processing, except in cases where such consent is not required by law.
- The processing is necessary to safeguard the vital interests of the Data Subject and the Data Subject is physically or legally incapacitated. In these events, the legal representatives must grant their authorisation.

- The processing is carried out in the course of legitimate activities and with due guarantees by a foundation, NGO, association or any other non-profit organisation, whose purpose is political, philosophical, religious or labour union, provided that it relates exclusively to its members or to persons who are in regular contact with them by reason of their purpose. In these events, the data may not be provided to third parties without the Data Subject authorisation.
- The processing relates to data which are necessary for the establishment, exercise or defence of a right in legal proceedings.
- The processing has a historical, statistical or scientific purpose. In this event, the measures leading to the deletion of the identity of the Data Subjects must be adopted.

7. Data Controller

The Data Controller of the databases covered by this policy is the FUNDACIÓN EDUCATIVA DE INGLATERRA, whose contact details are as follows:

- Address: AV CL 170 15 68, Toberín
- E-mail: contactenos@englishschool.edu.co
- Telephone: (601) 6767700.

8. Rights of the Data Subjects

The right to Data Protection aims to allow all individuals to know, update and rectify the information that has been collected about them in files or databases. This right is framed within Article 8 of the Data Protection Law and Chapter 25 section 4 of decree 1074 of 2015, the Data Subjects can exercise a series of rights in relation to the processing of their personal data. These rights may be exercised by the following persons:

1. By the Data Subject, who must provide sufficient proof of his or her identity by the various means made available to him or her by the Data Controller.
2. By their assignees, who must provide proof of such status.
3. By the representative and/or attorney-in-fact of the Data Subject, upon accreditation of the representation or power of attorney.
4. By stipulation in favour of another and for another.

The rights of children or adolescents shall be exercised by the persons who are empowered to represent them. The rights of the Data Subject are as follows:

- Right of access or consultation: This is the Data Subject's right to be informed by the Data Controller, upon request, regarding the origin, use and purpose of his or her personal data.

- Complaints and grievances rights. The law distinguishes between four types of complaints:
 - Claim for correction: The Data Subject's right to have partial, inaccurate, incomplete, fractioned, misleading or incomplete data, or data whose processing is expressly prohibited or has not been authorised, updated, rectified or modified.
 - Claim for deletion: The Data Subject's right to have data that is inadequate, excessive or does not respect constitutional and legal principles, rights and guarantees deleted.
 - Revocation claim: The right of the Data Subject to withdraw the authorisation previously given for the processing of his or her personal data.
 - Infringement complaint: the right of the Data Subject to request that a breach of Data Protection rules be remedied.
- Right to request proof of the authorisation granted to the Data Controller: Except when expressly exempted as a requirement for the processing in accordance with the provisions of Article 10 of the Data Protection Law.
- Right to file complaints before the Superintendence of Industry and Commerce regarding infringements: The Data Subject or assignee may only file this complaint once he/she has exhausted the consultation or complaint procedure before the Data Controller or Data Processor.

9. Attention to Data Subjects

The Head of School-Rector will be in charge of assigning the person who will deal with requests, queries and complaints, to whom the Data Subject can exercise his/her rights, at the following e-mail address: contactenos@englishschool.edu.co.

10. Functions and duties

10.1. Data Controller

The data security obligations of the FUNDACIÓN EDUCATIVA DE INGLATERRA are as follows:

- Coordinate and implement the security measures contained in this handbook.
- Disseminate this document to the staff involved.
- Keep the security measures updated and reviewed whenever relevant changes occur in the information system, the processing system, the organisation of the institution, the content of the information in the databases, or as a result of the periodic checks carried out. Similarly, their

content shall be reviewed whenever there is any change that may affect compliance with the security measures.

- Designate one or more security officers and identify the users authorised to access the databases in the handbook.
- Ensure that access through computer systems and applications is carried out by means of identified access and passwords.
- Authorise, unless expressly delegated to authorised users identified in the security measures, the output of media outside the establishments where the databases are located; the input and output of information by network, by means of electronic or paper storage devices and the use of modems and data downloads.
- Verify every six months the correct application of the backup and recovery procedure.
- Ensure the existence of a list of authorised users and user profiles.
- Analyse, together with the relevant Security Officer, the incidents recorded in order to establish the appropriate corrective measures, at least every two months.
- Conduct an internal or external audit to verify compliance with data protection security measures at least annually.

10.2. Security Officers

Security officers have the following functions:

- Coordinate and control the implementation of security measures, and collaborate with the Data Controller in the dissemination of security measures.
- Coordinate and monitor the mechanisms for accessing the information contained in the databases and prepare a regular report on such monitoring.
- Manage data access permissions for authorised users identified in the security measures.
- Enable the incident log for all users to report and record incidents related to data security as well as to agree with the Data Controller on corrective measures and record them.
- Periodically check the validity and currency of the list of authorised users, the existence and validity of backup copies for data recovery, the updating of security measures and compliance with measures related to data input and output.
- Define the timeframe within which audits are to be carried out, which may not exceed one year.
- Receive and analyse the audit report in order to raise its conclusions and propose corrective measures to the controller.
- Manage and control incoming and outgoing records of documents or media

containing personal data.

10.3. Users

All persons involved in the storage, processing, consultation or any other activity related to the personal data and information systems of the FUNDACIÓN EDUCATIVA DE INGLATERRA must act in accordance with the functions and obligations set out in this section.

The FUNDACIÓN EDUCATIVA DE INGLATERRA complies with the duty of information by including confidentiality agreements and the duty of secrecy subscribed to, where applicable, by users of identification systems on databases and information systems, and by means of an informative circular addressed to them.

The functions and obligations of the staff of the FUNDACIÓN EDUCATIVA DE INGLATERRA are defined in general terms, according to the type of activity they carry out in accordance with their functions within the institution and, specifically, by the content of this handbook. The list of users and profiles with access to protected resources is contained in the security measures set out in this handbook. When a user processes documents or media containing personal data, he/she has the duty to safeguard them, as well as to monitor and control that unauthorised persons cannot have access to them.

Non-compliance with the obligations and security measures established in this handbook by staff in the service of the FUNDACIÓN EDUCATIVA DE INGLATERRA is punishable in accordance with the regulations applicable to the legal relationship existing between the user and the FUNDACIÓN EDUCATIVA DE INGLATERRA.

The functions and obligations of the users of the personal databases, under the responsibility of the FUNDACIÓN EDUCATIVA DE INGLATERRA, are the following:

1. Duty of secrecy: Applies to all persons who, in the development of their profession or work, access personal databases and links both users and contracted service providers in compliance with this duty. Users of the FUNDACIÓN EDUCATIVA DE INGLATERRA, may not communicate or disclose to third parties, data they handle or of which they have knowledge in the performance or position of their duties, and must ensure the confidentiality and integrity of the same.
2. Control functions and delegated authorisations: The Data Controller may delegate the processing of data to a third party, to act as a Data Processor, by means of a data transfer contract.
3. Obligations related to the security measures in place:

- Access databases only with proper authorisation and when necessary for the exercise of their functions.
 - Do not disclose information to third parties or unauthorised users.
 - Observe safety standards and work to improve them.
 - Do not perform actions that pose a danger to the security of the information.
 - Not to remove, move and provide information from the organisation's premises without proper authorisation.
4. Use of work resources and materials: must be oriented to the exercise of the assigned functions. The use of these resources and materials for personal purposes or for purposes unrelated to the tasks corresponding to the workstation is not authorised. When, for justified work-related reasons, it is necessary to remove peripheral or removable devices, the corresponding security officer must be notified and may authorise and, where appropriate, record it.
 5. Use of printers, scanners and other copying devices: When using these types of devices, copies should be collected immediately, avoiding leaving them in their trays.
 6. Obligation to notify incidents: Users are obliged to notify any incidents of which they become aware to the relevant Security Officer, who will be responsible for their management and resolution. Some examples of incidents are: the failure of the computer security system that allows access to personal data by unauthorised persons, unauthorised attempts to remove a document or medium, loss of data or total or partial destruction of media, change of physical location of databases, knowledge of passwords by third parties, modification of data by unauthorised staff, etc.
 7. Duty of custody of the media used: Obliges the authorised user to monitor and control unauthorised persons accessing the information contained on the media. The media containing databases must identify the type of information they contain by means of a labelling system and be inventoried. When the information is classified at a sensitive security level, the labelling system must only be understandable to users authorised to access such information.
 8. Responsibility for work terminals and laptops: Each user is responsible for his or her own work terminal. When absent from work, he or she must lock the terminal (e.g. screen saver with password) to prevent viewing or accessing the information it contains; and he or she must switch off the terminal at the end of the working day. Laptops must also be monitored at all times to prevent loss or theft.
 9. Limited use of the Internet and e-mail: The sending of information electronically and the use of the Internet by staff is limited to the performance of their activities.
 10. Safeguarding and protection of passwords: The passwords provided to users are personal and non-transferable, and therefore, their disclosure or communication to unauthorised persons is prohibited. When the user accesses for the first time with the assigned password, it is necessary to change it. When it is

necessary to reset the password, the user must inform the System Administrator. Users must change their password when instructed to do so by the system or on a regular basis.

11. Data backup and recovery: All information in the institution's personal databases should be backed up.

12. Duty to archive and manage documents and media: Documents and media must be properly archived with the security measures set out in the Policies and Procedures handbook.

11. Procedures for exercising the Data Subject's rights

11.1. Right of access or consultation

According to Chapter 25, Section 4 of Decree 1074 of 2015 and Decree 1074 of 2015, the Data Subject may consult his or her personal data free of charge in two cases:

1. At least once every calendar month.
2. Whenever there are substantial modifications to the information processing policies that give rise to new consultations.

For consultations whose periodicity is greater than one per calendar month, the FUNDACIÓN EDUCATIVA DE INGLATERRA may only charge the Data Subject for the costs of sending, reproduction and, where appropriate, certification of documents. Reproduction costs may not exceed the costs of recovery of the corresponding material. For this purpose, the responsible party must demonstrate to the Superintendence of Industry and Commerce, when required, the support of such expenses.

The Data Subject may exercise the right of access or consultation of his/her data by writing to the FUNDACIÓN EDUCATIVA DE INGLATERRA, sent by e-mail, indicating in the subject "exercise of the right of access or consultation". The request must contain the following data:

- Name and surname of the Data Subject.
- Photocopy of the Data Subject's Citizenship Card and, if applicable, of the person representing the Data Subject, as well as the document accrediting such representation.
- Request in which the request for access or consultation is made.
- Address for notifications, date and signature of the applicant.
- Documents accrediting the request made, where applicable.

The Data Subject may choose one of the following ways of consulting the database in order to receive the requested information:

- On-screen display.
- In writing, with copy or photocopy sent by registered or unregistered mail.
- Mail or other electronic means.
- Another system appropriate to the configuration of the database or the nature of the processing, offered by the FUNDACIÓN EDUCATIVA DE INGLATERRA.

Once the request has been received, the FUNDACIÓN EDUCATIVA DE INGLATERRA will resolve the consultation request within a maximum period of ten (10) working days from the date of receipt of the request. If it is not possible to deal with the consultation within this period, the interested party will be informed, stating the reasons for the delay and indicating the date on which the consultation will be dealt with, which in no case may exceed five (5) working days following the expiry of the first period. These deadlines are set out in Article 14 of the Data Protection Law.

Once the consultation procedure has been exhausted, the Data Subject or assignee may file a complaint with the Superintendence of Industry and Commerce.

11.2. Complaints and grievances rights

The Data Subject may exercise his/her right to complain about his/her data by sending a letter to the FUNDACIÓN EDUCATIVA DE INGLATERRA by e-mail to contactenos@englishschool.edu.co, indicating in the subject line "Exercise of the right to complaint or claim", the request must contain the following data:

- Name and surname of the Data Subject.
- Photocopy of the Data Subject 's Citizenship Card and, if applicable, of the person representing the Data Subject, as well as the document accrediting such representation.
- Description of the facts and the request for correction, deletion, revocation or inflation.
- Address for notifications, date and signature of the applicant.
- Documents accrediting the request made that are to be asserted, where applicable.

If the claim is incomplete, the interested party will be required within five (5) days of receipt of the claim to rectify the faults. After two (2) months from the date of the request, without the applicant submitting the required information, it will be understood that the claim has been withdrawn.

Once the completed complaint has been received, a legend will be included in the database stating "complaint in process" and the reason for the complaint, within a

period of no more than two (2) working days. This legend must be maintained until the complaint is decided.

The FUNDACIÓN EDUCATIVA DE INGLATERRA will resolve the request for consultation within a maximum period of fifteen (15) working days from the date of receipt. When it is not possible to respond to the claim within this period, the interested party will be informed of the reasons for the delay and the date on which the claim will be addressed, which in no case may exceed eight (8) working days following the expiration of the first term.

Once the complaint process has been exhausted, the Data Subject or assignee may file a complaint with the Superintendence of Industry and Commerce.

12. Infringements and penalties

According to Chapter II of the Statutory Law 1581 of 2012 on Data Protection, the Superintendence of Industry and Commerce may impose sanctions for non-compliance with data protection regulations on the Data Controller or Data Processor. The possible sanctions are:

- Fines of a personal and institutional nature up to the equivalent of two thousand (2,000) legal monthly minimum salaries in force at the time the sanction is imposed. Fines may be successive as long as the non-compliance that gave rise to them persists.
- Suspension of treatment-related activities for up to six (6) months. The act of suspension shall indicate the corrective measures to be taken.
- Temporary closure of the operations related to the processing once the term of suspension has elapsed without the corrective measures ordered by the Superintendence of Industry and Commerce having been adopted.
- Immediate and definitive closure of the operation involving the processing of sensitive data.

13. Security measures

The FUNDACIÓN EDUCATIVA DE INGLATERRA, in order to comply with the principle of security enshrined in Article 4 (g) of the Data Protection Law has implemented technical, human and administrative measures necessary to ensure the security of the records avoiding their adulteration, loss, consultation, use or unauthorised or fraudulent access.

On the other hand, the FUNDACIÓN EDUCATIVA DE INGLATERRA, through the subscription of the corresponding transmission contracts, has required the Data Processors with whom it works to implement the necessary security measures to guarantee the security and confidentiality of the information in the processing of personal data.

The security measures implemented by the FUNDACIÓN EDUCATIVA DE INGLATERRA, which are included and developed in this handbook (Tables II, III, IV and V), are set out below.

Table II. Common security measures for all types of data (public, semi-private, private, sensitive) and databases (automated, non-automated)

Audit	Document management and supports	Access control	Incidents	Staff	Security handbook
1. Regular audit (internal or external) every year. 2. Any extraordinary audits due to substantial changes in the information systems. 3. Report on the detection of deficiencies and proposal for corrections. 4. Analysis and conclusions of the Security Officer and the Data Controller. 5. Retention of the report at the disposal of the authority.	1. Measures such as paper shredders that prevent improper access to or recovery of data that has been discarded, erased or destroyed. 2. Restricted access to the place where the data is stored. 3. Authorisation of the person responsible for the output of documents or media by physical or electronic means. 4. System of labelling or identification of the type of information. 5. Inventory of the media on which databases are stored.	1. User access limited to the data necessary for the development of their functions, according to their role. 2. Updated list of authorised users and accesses. 3. Written authorisation from the Data Subject for the release of his or her data to third parties, in order to prevent access to data with rights other than those authorised. Granting, alteration or cancellation of permits by authorised staff.	1. Incident register: type of incident, time of occurrence, sender of the notification, recipient of the notification, effects and corrective measures. 3. Incident notification and management procedure.	1. Definition of roles and obligations of users with access to data. 2. Definition of the control functions and authorisations delegated by the Data Controller. 3. Dissemination among staff of the rules and the consequences of non-compliance with the rules.	1. Elaboration and implementation of the mandatory staff handbook. 2. Minimum content: scope of application, security measures and procedures, roles and obligations of staff, description of databases, incident procedure, data copying and recovery procedure, security measures for the transport, destruction and re-use of documents, identification of Data Processors.

Table III. Common security measures for all types of data (public, semi-private, private, sensitive) according to type of databases

Non-automated databases			Automated databases	
Archive	Document storage	Custody of documents	Identification and authentication	Telecommunications
1. Archiving of documentation following procedures that guarantee correct conservation, location	1. storage devices with mechanisms to prevent access by unauthorised persons.	1. Duty of care and custody of the person in charge of documents	1. Personalised identification of users to access information systems and	1. Access to data through secure networks.

and consultation and the exercise of the rights of the Data Subjects.		during the review or processing of documents.	verification of their authorisation. 2. Identification and authentication mechanisms; Passwords: assignment, expiry and encrypted storage.	
---	--	---	--	--

Table IV. Security measures for private data according to the type of databases

Automated and non-automated databases			Automated databases			
Audit	Security Officer	Security handbook	Document and support documents management	Access control	Identification and authentication	Incidents
1. Regular audit (internal or external) every year. 2. Extraordinary audits due to substantial changes in the information systems. 3. Report on the detection of deficiencies and proposal for corrections. 4. Analysis and conclusions of the Security Officer and the Data Controller. 5. Retention of the Report at the disposal of the authority	1. Designation of one or more Security Officers. 2. Designation of one or more persons responsible for the control and coordination of the measures in the handbook. 3. Prohibition of delegation of the Data Controller's responsibility to the Security Officer.	1. Compliance checks at least once a year, consisting of the annual audit, as well as staff training at least once a year.	1. Register of incoming and outgoing documents and support documents: date, sender and receiver, number, type of information, form of dispatch, person responsible for receipt or delivery.	1. Controlling access to the site(s) where information systems are located.	1. Mechanism to limit the number of repeated unauthorised access attempts.	1. Logging of data recovery procedures, person performing the procedures, data restored and data manually recorded. 2. Authorisation of the Data Controller for the execution of recovery procedures.

Table V. Security measures for sensitive data according to type of databases

Non-automated databases				Automated databases		
Access control	Document storage	Copying or reproduction	Transfer of documentation	Document and support documents management	Access control	Communications
1. Access for authorised staff only. 2. Access identification mechanism. 3. Logging of unauthorised user access.	1. Filing cabinets, cupboards or other cabinets located in access areas protected by keys or other measures.	1. Only by authorised users. 2. Destruction that prevents access to or recovery of data.	1. Measures to prevent access to or manipulation of documents.	1. Confidential labelling system. 2. Data encryption. 3. Encryption of portable devices when going outside.	1. Access log: user, time, database accessed, type of access, record accessed. 2. Control of the access log by the security officer. Monthly report. 3. Data retention: for the period of time required by law. imposed.	1. Data transmission via encrypted electronic networks.

14. Navigation data

The navigation system and the software necessary for the operation of this website collect some personal data, the transmission of which is implicit in the use of Internet communication protocols.

By its very nature, the information collected could allow the identification of users through its association with third party data, although it is not obtained for that purpose. This category of data includes the IP address or domain name of the computer used by the user to access the website, the URL address, the date and time and other parameters relating to the user's operating system.

This data is used for the sole purpose of obtaining anonymous statistical information on the use of the website or to check its correct technical functioning, and is deleted immediately after verification.

15. Cookies or web bugs

This website does not use cookies or web bugs to collect the user's personal data; their use is limited to facilitating the user's access to the website. The use of session cookies, which are not permanently stored on the user's computer and disappear when the browser is closed, is limited solely to collecting technical information to identify the session in order to facilitate secure and efficient access to the website. If you do not wish to allow the use of

cookies, you can reject them or delete existing ones by configuring your browser and disabling the browser's Java Script code in the security settings.

16. Transfer of data to third countries

According to Title VIII of the Data Protection Law, the transfer of personal data to countries that do not provide adequate levels of data protection is prohibited. It is understood that a country offers an adequate level of data protection when it complies with the standards set by the Superintendence of Industry and Commerce on the matter in accordance with Circular 005 of 10 August 2017, which in no case may be lower than those required by this law for its recipients.

This prohibition shall not apply in the case of:

- Information in respect of which the Data Subject has given his or her express and unequivocal authorisation for the transfer.
- Exchange of medical data, when so required for the processing of the Data Subject for reasons of public health or hygiene.
- Bank or stock exchange transfers, in accordance with the legislation applicable to them.
- Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.
- Transfers necessary for the performance of a contract between the Data Subject and the Data Controller, or for the performance of pre-contractual measures, subject to the Data Subject's consent.
- Transfers legally required for the safeguarding of the public interest, or for the recognition, exercise or defence of a right in legal proceedings.

In cases not covered by the exception, the Superintendency of Industry and Commerce shall be responsible for issuing the declaration of conformity regarding the international transfer of personal data. The Superintendent is empowered to request information and to carry out the necessary steps to establish compliance with the requirements for the viability of the operation.

International transfers of personal data between a Data Controller and a Data Processor to enable the Data Processor to carry out processing on behalf of the Data Controller do not require the Data Subject's notice and consent, provided that a contract for the transfer of personal data is in place.

17. Related policies

- Bylaws of the Fundación Educativa de Inglaterra
- Corporate Governance Handbook

- Coexistence Handbook
- Internet Acceptable Use Policy
- Policy for Teaching and Learning with Information and Communication Technologies (ICT) in the TES Community

18. Approval and details for review

Approval and Review	Details
Approving authority	Board of Directors
Committee or working group that submits it to the approving authority	Secretary-General
Administrator	Board of Directors/ Head of School-Rector / Secretary-General
New Date for review	April 2022

19. Validity

The databases under the responsibility of the FUNDACIÓN EDUCATIVA DE INGLATERRA will be subject to processing for the time that is reasonable and necessary for the purpose for which the data are collected. Once the purpose or purposes of the processing have been fulfilled, and without prejudice to legal regulations that provide otherwise, the FUNDACIÓN EDUCATIVA DE INGLATERRA will proceed to delete the personal data in its possession unless there is a legal or contractual obligation that requires its conservation. For all these reasons, this database has been created to come into effect with the approval given by the Board of Directors, without a defined period of validity, but will be modified when the regulation so provides and/or when the management body deems it necessary.

This policy was approved by the Board of Directors on 28th May 2021 and will become effective upon approval.

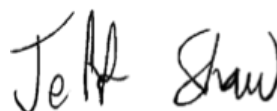
20. Version Control

VERSION	DATE			TRACEABILITY OF CHANGE
01	01	01	2013	• Version 1
02	28	05	2021	• Version 2



WATSON LAWRENCE VARGAS

President of the Board of Directors



JEFFREY NIGEL SHAW

Head of School / Rector