Data Protection Policy

Smart INTL College

Introduction

This Policy sets out the obligations of Smart INTL College regarding data protection and the rights of customers and business contacts ("data subjects") in respect of their personal data.
This Policy sets the college's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the SMAT INTL College, its employees, agents, contractors, or other parties working on behalf of the college.

The Data Protection Principles

All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

The Rights of Data Subjects

- The right to be informed'
- The right of access,
- The right to rectification,
- The right to erasure,
- The right to restrict processing,
- The right to data portability,
- The right to object; and
- Rights with respect to automated decision-making and profiling.

Lawful, Fair, and Transparent Data Processing

All personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's health), at least one of the following conditions must be met:
- The data subject has given their explicit consent to the processing of such data for one or more specified purposes;

- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The processing relates to personal data which is clearly made public by the data subject;

Specified, Explicit, and Legitimate Purposes
The college collects and processes the personal data set out in this Policy.
This includes:

- Personal data collected directly from data subjects **OR**
- Personal data obtained from third parties.
- The college only collects, processes, and holds personal data for the specific purposes set out in this Policy.
- Data subjects are kept informed at all times of the purpose or purposes for which the college uses their personal data.

Adequate, Relevant, and Limited Data Processing
The college will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

Accuracy of Data and Keeping Data Up-to-Date

- The College shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.
- The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Data Retention

- Smart INTL College shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- For full details of the College's approach to data retention, including retention periods for specific personal data types held by the College, please refer to our Data Retention Policy.

Secure Processing
The college shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided later in this Policy.

Accountability and Record-Keeping
The college's Data Protection Officer is [Matav Ardalan],
E-Mail: [office.coordinator@smart-international.org]
Tel: [00964 750 114 7235].

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy.

- The college shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
- The name and details of the college, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the college collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the college, and the categories of data subject to which that personal data relates;
- Details of how long personal data will be retained by the college; and
- Detailed descriptions of all technical and organisational measures taken by the Smart INTL College to ensure the security of personal data.

Data Protection Impact Assessments

- The college shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.
- Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
  1. The type(s) of personal data that will be collected, held, and processed;
  2. The purpose(s) for which personal data is to be used;
  3. The college's objectives;
  4. How personal data is to be used;
  5. The parties (internal and/or external) who are to be consulted;
  6. The necessity and proportionality of the data processing with respect to the
  7. purpose(s) for which it is being processed;
  8. Risks posed to data subjects;
  9. Risks posed both within and to the college; and
  10. Proposed measures to minimize and handle identified risks.

Keeping Data Subjects Informed

The college shall provide the information set out in section (i) below to every data subject:
Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
a) if the personal data is used to communicate with the data subject, when the first communication is made; or
b) if the personal data is to be transferred to another party, before that transfer is made; or
c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

(i) The following information shall be provided:

- Details of the college including, but not limited to, the identity of its Data Protection Officer;
- The purpose(s) for which the personal data is being collected and will be processed (as detailed in this Policy);
- Where applicable, the legitimate interests upon which the college is justifying its collection and processing of the personal data;
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- Where the personal data is to be transferred to one or more third parties, details of those parties.

Data Subject Access

- Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the college holds about them, what it is doing with that personal data, and why.
- Data subjects wishing to make a SAR may do so in writing. SARs should be addressed to the college's Data Protection Officer at [Smart INTL College]., [Office#7, Tower 4, floor 11, Empire Business Towers, Erbil, Iraq] Tel: [00964 750 520 0052]
  Email:[info@smartexpertiraq.com]
- Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- All SARs received shall be handled by the college's Data Protection Officer.
- The College does not charge a fee for the handling of normal SARs. The college reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data

- Data subjects have the right to require the college to rectify any of their personal data that is inaccurate or incomplete.
- The college shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the college of the issue.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data
Data subjects have the right to request that the college erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
b) The data subject wishes to withdraw their consent to the college holding and processing their personal data;

Unless the college has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request.

Restriction of Personal Data Processing
Data subjects may request that the college ceases processing the personal data it holds about them. If a data subject makes such a request, the college shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

Data Security - Transferring Personal Data and Communications
The college shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be encrypted using Encryption software;
- All emails containing personal data must be marked "confidential";
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted using deletion software;
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

Data Security - Storage
The college shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords and data encryption;
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically should be backed up at least daily with backups stored onsite. All backups should be encrypted using data encryption'
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the college or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the college where the party in question has agreed to comply fully with the letter and spirit of this Policy.

Data Security - Disposal
When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

Data Security - Use of Personal Data
The college shall ensure that the following measures are taken with respect to the use of personal data:

- No personal data may be shared informally and if an employee, any other party working on behalf of the college that requires access to any personal data that they do not already have access to, such access should be formally requested from The Data Protection Officer,
- No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the college or not, without the authorisation of The Data Protection Officer,
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
- Where personal data held by the college is used for marketing purposes, it shall be the responsibility of The Data Protection Officer to ensure that the appropriate consent is obtained.

Data Security - IT Security

Smart INTL college ensures that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the college, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The IT staff shall be responsible for installing any and all security-related updates after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so; and
- No software may be installed on any computer or device without the prior approval of the college.

Organisational Measures

The college shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the college shall be made fully aware of both their individual responsibilities and the college's responsibilities under this policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the college;
- All employees, agents, contractors, or other parties working on behalf of the college handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

Data Breach Notification

- All personal data breaches must be reported immediately to the Data Protection Officer.
- If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the college board of directors is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- Data breach notifications shall include the following information:
  - The categories and approximate number of data subjects and personal data records concerned;
  - The name and contact details of the college's data protection officer;
  - The likely consequences of the breach;
  - Details of the measures taken, or proposed to be taken, by the college to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

This policy has been approved & authorised by:

Name: Awaz Ahmad Shikhi

Position: Regional Director

Date: 16 March 2021

Signature: 

Review of Policy: March 2022