



**THE BRITISH SCHOOL OF MILAN**  
LEARNING TO EXCEL SINCE 1969

## GDPR & DATA PROTECTION POLICY

The purpose of this document is to regulate the use of IT equipment for the people in charge of these services (hereinafter *Delegate*) within *The British School of Milan S.r.l* and *The Sir James Henderson British School of Milan* (hereinafter *BSM*).

These security rules have the objective of providing the *Delegate* with appropriate security measures and appropriate behaviour guidelines to use the company e-mail, internet browsing and data processing held by *BSM* in a compliant and non-risky way.

Given that the use of corporate IT resources must always be based on the principle of diligence and correctness, this Policy is adapted in compliance with the rules issued by the EU Regulation 2016/679 (GDPR) for the protection of personal data.

A copy of this Policy is given to each employee and to each third party at the beginning of the activity with *BSM*.

### **Introduction**

The continued increasing spread of new information technologies and in particular the free access to Internet through Personal Computers, exposes *BSM* to the risks of both patrimonial and penal involvement, creating problems to the security and the image of *BSM* itself.

This document meets the need to regulate the ways for the correct use of IT equipment by employees and collaborators and contains useful information to understand what each *Delegate* can do to help ensure the IT security of the whole *BSM*.

### **Field of application**

This Policy applies:

- To all the employees and all third parties of *BSM* (hereinafter jointly called *Delegates*) who are working on the personal data owned by *BSM*;
- To all activities or behaviours in any case connected to the use of the Internet and e-mail, through company or third-party tools authorized to use by *BSM*.

### **Regulatory requirements and definitions**

The *Delegates* are the authorized persons, by the Data Holder (*BSM*), to carry out data processing operations. In particular, processing operations may only be carried out by *Delegates* who operate under the direct authority of *BSM*, following the instructions received.

For the purposes of this Policy, we point out that:

- The term "*treatment*" refers to any operation performed on data with or without the aid of automated means that has as its object the collection, registration, consultation, processing, modification, spread, extraction, destruction of data even if not registered in the database;



## GDPR & DATA PROTECTION POLICY

- The term "*personal data*" refers to any information concerning a person or legal entity, whether it is nominative information or any other information that can make the person or the entity identifiable;
- The term "*sensitive data*" refers to data suitable for detecting racial and ethnic origin, philosophical or other religious convictions, political opinions, membership of parties, trade unions, religious associations and organizations, philosophical, political or trade union, as well as personal data suitable for detecting the state of health and sexuality of the person/entity concerned;
- The term "*judicial data*" refers to the data suitable for detecting the provisions concerning criminal records, the register of administrative penalties for crimes and the related pending charges.

As stated at art. 12 of the BSM Regulations Booklet the School, as the body responsible for data processing, will responsibly process Students, Teachers and Parents personal data and the data of the subjects to whom the Request for Registration applies, **identification** data (including: name, address, fiscal code) and **sensitive** (illness or health conditions or intolerances or allergies) in compliance with European Regulation (GDPR) 2016/679.

By signing the Acceptance Form, identification data are also processed without the express consent of the Applicant and the Member for the following **Academic Purposes**: execution of the Request for Registration; management of pre-contractual and contractual relationships; tax compliance, management of receipts and payments; the obligations imposed by laws, regulations or legislation or imposed by the Authority for the execution of the Contract.

The Applicants Identification and non-sensitive data are processed only after their distinct and explicit consent, for the following Purposes of Promoting and Enhancing the School:

- 1) emailing the school newsletter to the Parents and Students containing information, including promotional and related school events and activities organized by the same;
- 2) photographic image publication and / or videos of the students, taken or recorded during internal or external events organized at the school by the school, and / or the name (never the image and the name together) of the subjects themselves, the brochure and / or School promotions and / or within the Website and social accounts of the School. This has the sole purpose of promoting the school and developing its profile.

The data will be made available for purposes of the points above, to employees and consultants of the School, including the Members who perform the role of Class Representatives, in their capacity as data processors; to the organization of Members called "Friends of the School" and to organizations working on behalf of the School, in their capacity as data processors and / or system administrators.

The list of data processed, the tools used, the criteria used for saving and restoring data are summarized in the Security Policy Document and in the Register of treatments carried out.



## GDPR & DATA PROTECTION POLICY

### **Guidelines**

BSM holds the personal data of its students, including: details of the enrolment contract, evaluation / examination results, information on attendance, positive and negative behaviour and characteristics such as ethnic group, special educational needs, medical information and photographs.

The data is used to manage the educational activity of the students, to provide adequate pastoral support and to evaluate the overall performance of BSM.

Any use of personal data relating to students, their parents or fundraising, advertising or promotion must be done with the explicit consent of the interested party.

The following describes the rules to which the *Delegates* must abide in carrying out the tasks involving the processing of personal data referring to both persons and legal entities.

First of all it should be noted that, in order to prevent outsiders from knowing the personal data being processed, the *Delegate* must observe the following rules of ordinary diligence, as well as any other measures deemed necessary to ensure compliance with the provisions from the legislation:

- All processing operations must be carried out in such a way as to ensure compliance with the security measures, the utmost confidentiality of the information that is in possession assuming that all data are confidential and subject to professional secrecy;
- The individual phases of work and the behaviour to be applied must make it possible to avoid the data being subject to risk of loss or destruction, that unauthorized persons can access it, and that the processing operations carried out are only the authorized one and in compliance with the authorized scope;
- In the event of moving away, even temporarily, from the workplace, all necessary measures must be taken to ensure that third parties, even if they are employees, can not access personal data for which treatment (automated or in paper) is in progress;
- Only operations in compliance with the tasks assigned by the direct manager must be carried out;
- Only the processing operations necessary to achieve the purposes for which the data is collected must be carried out;
- The accuracy of the data processed and the relevance to the objectives pursued in the individual cases must be constantly verified.

### **Access to data from the workstation**

The use of the PC and of the company network must be carried out by meeting the following rules:

- The PC entrusted to the *Delegate* is a work tool; everyone is responsible for the use of the IT equipment received and its use must be for purposes related to their work (tasks) only
- The user is not allowed to modify the hardware and software features set on each PC, unless authorized by the CFO
- If you have a Laptop, do not leave it unattended
- Do not leave smartphones and tablets unattended
- Information/data digitally stored must be exclusively needed for the work activity and only upon express authorization of the direct manager



## GDPR & DATA PROTECTION POLICY

- Do not connect USB keys to BSM work stations
- Do not download company documents on your personal PC
- Do not open company documents from your personal PC
- Do not use your personal devices to take pictures or movies of BSM students
- It is forbidden to install any software on the company PC independently; there is a serious danger of introducing viruses and / or of altering the functionality of existing software applications and of violating copyright law by not having the appropriate licenses purchased by BSM.
- Do not leave confidential information on the desk wherever it is stored
- Do not use fax and / or telephone to forward confidential and personal information if you are not absolutely sure of the identity of the interlocutor or of the addressee and if you are absolutely sure (s)he is legitimated to receive them
- It is forbidden to use the company network for purposes not expressly authorized
- It is forbidden to connect workstations to the network if not under the explicit and formal authorization of the CFO
- Unauthorized installation of modems that exploit the telephone communication system for access to external or internal BSM databases is prohibited
- It is forbidden to share folders on the network with or without a password, unless explicitly and formally authorized by the CFO
- The System Administrator can, upon express authorization of the CFO, proceed with the removal of any file or application that he considers to be dangerous for security both on the PCs of the *Delegate* and on the network units.

### **Password management**

Access to the company network is password protected; for access, must be used the personal profile (username and password) assigned by the System Administrator who also manages the deadlines and the characteristics of the password.

For correct password management, each *Delegate* must take care of:

- Keep it confidential and do not disclose it to third parties
- Do not allow other employees to operate with your own profile
- The *Delegate* is required to lock the PC whenever (s)he leaves the room where the PC is located temporarily or logout when leaving a classroom

Leaving an unlocked PC / device connected to the network can allow the use by third parties without the possibility of proving its improper use afterwards.

### **Internet and e-mail**

Internet and e-mail must be used exclusively for work purposes. Behaviours that may cause damage to BSM is prohibited. The e-mail box assigned by BSM to the *Delegate* is a work tool, the assignees of the e-mail boxes are responsible for the correct use of the same.



## GDPR & DATA PROTECTION POLICY

Enabling the use of e-mail and browsing Internet is expressly authorized by the CFO.

In particular, the *Delegate* must observe the following rules:

- In the case of unknown senders or unusual messages you will need to delete the messages without opening them in order not to run the risk of being infected by viruses
- It is forbidden to use e-mail to communicate confidential information, personal data or critical data without being confident that the data is protected.
- It is always necessary to make sure that recipients of correspondence by e-mail are authorized to get the data that will be sent
- The mailbox should be kept in order by deleting unnecessary documents and deleting cumbersome attachments
- It is not allowed to register on internet sites or to participate in blogs if this is not strictly necessary for carrying out the required job.

### **Antivirus protection**

The PCs assigned by BSM to the *Delegates*, while protected against the attacks of viruses by installation of appropriate and sophisticated software, remain potentially exposed to attacks by unknown viruses.

To reduce the probability of these attacks, the following rules must be met:

- Close the programs in use correctly
- If you are working on the network, do not open suspicious or dubious files
- Do not download or install applications / software that have not been previously authorized
- Do not use devices/tools of uncertain origin
- Pay the necessary attention to any anomalous signals sent by the PC during data processing activity.

If you note a malfunction of the PC which can make you suspect the presence of viruses, the *Delegate should*:

- Suspends any activity on the PC
- Closes the work and the linked applications
- Contacts the System Administrator immediately

### **Data Breach**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed. Examples of a data breach could include the following:

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss)
- Inappropriate access controls allowing unauthorised use
- Human error (for example sending an email or SMS to the wrong recipient)
- Hacking, phishing and other attacks where information is obtained by deceiving whoever holds it





## GDPR & DATA PROTECTION POLICY

In the case of suspected or confirmed violation of personal data, any employee must report it to:

- the Chief Financial Officer, Gianni Iaia, [gianni.iaia@bsm.school](mailto:gianni.iaia@bsm.school)
- the ICT Director, Andrea Lanuara, [andrea.lanuara@bsm.school](mailto:andrea.lanuara@bsm.school)

Upon receipt of the report, the CFO and the ICT Director will carry out further in-depth investigations and discuss them with the DPO Mr Roberto Ferri ([dpo@bsm.school](mailto:dpo@bsm.school))

It will be the responsibility of the DPO to establish whether a personal data breach has in fact occurred, and evaluate if any specific communication to the Authority is needed.

BSM will then identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. BSM will identify ways to recover, correct or delete data (for example notifying the police if the breach involves stolen hardware or data).

### **Paper archives**

No paper material containing personal data should be left unattended on desks and, at the end of the work, it must be stored in a safe place. In addition, the same attention must be used in carrying out the normal daily work operations, to avoid the material being easily visible to third parties or in any case to those not authorized to receive it.

In the case of processing sensitive data, all paper documentation must be kept in locked cabinets / drawers or locked room in case of temporary moving away from the work station.

### **Access to user data**

The System Administrator can access the data processed by the *Delegate* by e-mail or surfing the net exclusively for reasons of security and protection of the IT system or for technical and / or maintenance reasons and / or regular work activities.

Except for urgent interventions that are necessary to deal with emergency situations and guarantee maximum security, the System Administrator will access the data at the request of the *Delegate* and / or after an appropriate notice to him/her. Where necessary to guarantee security, technical assistance and normal operations, the System Administrator will also have the option of connecting and viewing the individual work stations remotely. The System Administrator can, in the cases indicated above, proceed with all the configuration and management operations necessary to guarantee the correct functionality of the company IT system.

In case of sudden or prolonged absence of the *Delegate*, and due to urgent security needs and/or for system operation, the System Administrator is, upon the express authorization of the CFO, authorized to access the e-mail of the *Delegate*. Timely notice to the *Delegate* must, however, be given for any such access.



## GDPR & DATA PROTECTION POLICY

The System Administrator, after the express authorization of the CFO, can carry out checks on navigation aimed at ensuring the operation and safety of the system, as well as the necessary work activities. Any control of the log files by the System Administrator is not continuous and is limited to some information; the files are kept for the period strictly necessary to the pursuit of the organizational, productive and security objectives of BSM. In any case the files cannot be kept later than 12 months, without prejudice to specific legal obligations.

The log recording system is set to periodically and automatically delete (through overwriting procedures) the personal data of the *Delegate* used for internet access.

The System Administrator, after the express authorization of the CFO, is also authorized to access the data contained in the IT devices returned by the *Delegate* to BSM due to termination of the employment/relationship, replacement of equipment, etc. The prior cancellation of all personal data contained therein will be the responsibility of the *Delegate*.

In any case it is guaranteed that no activity is carried out using hardware and software systems specifically designed for remote control, such as, for example:

- Systematic reading and recording of e-mail messages or related external data (log) beyond what is technically necessary for carrying out the e-mail service;
- reproduction of any systematic memorization of the web pages opened by the *Delegate*;
- reading and recording of the characters entered via the keyboard or similar device.

### Using photographs of individual children

The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications
  - on the school website
  - in newspapers as allowed by the school
  - in videos made by the school or in class for school projects
  - on social media
- Images will be carefully chosen to ensure that they do not pose a risk of misuse.
- For public documents, including in newspapers, full names will not be published alongside images of the child.

### Right to access personal data

As stated in the Regulation Booklet art. 12.6, Parents and Students, will be able to access their data and that of the children to whom the Request for Registration applies at any time and exercise

their rights under art. 15 of GDPR 2016/679 which are visible at the bottom of this document. The Applicants and the Members will be able at any time to exercise their rights under art. 15 of GDPR 2016/679 by emailing [secretary@bsm.school](mailto:secretary@bsm.school).



## GDPR & DATA PROTECTION POLICY

BSM DATA PROCESSED: STUDENTS - PARENTS - EMPLOYEES			
<b>DATA/ DOC. STUDENT</b>	<b>Data / Doc destruction</b>	<b>DATA / DOC. EMPLOYEE</b>	<b>Data / Doc destruction</b>
Name and Last name	Archive	Name and Last name	10 years
Birth Certificate	End of academic relationship	Birth Certificate	End of academic relationship
Fiscal Code	Archive	Fiscal Code	10 years
Address of residency	10 years	Address of residency	10 years
Class	Archive	Medical info	End of academic relationship
Enrolment date	Archive	Vaxinations	End of academic relationship
Academic reports	Archive	Criminal record	End of academic relationship
Conduct reports	Archive	Curruculum Vitae	10 years
ID document	10 years	Marital data	End of academic relationship
Registration form	10 years	Children data	End of academic relationship
Medical info	End of academic relationship	Letter of appointment	10 years
Vaxinations	End of academic relationship	Letter of resignation	10 years
<b>DATA / DOC. PARENTS</b>		Letter of salary increase	10 years
		References	10 years
		Bank account	End of academic relationship
		House rent contract	End of academic relationship
		Passaport / ID doc	10 years
Name and Last name	10 years	Health card	10 years
Address of residency	10 years		
Mobile phone	End of academic relationship		
Email	End of academic relationship		
Assiciation registration form	10 years		
Custody documents	10 years		
Fiscal code	10 years		
ID document	10 years		

### **Controls by BSM**

It is emphasized that the IT equipment and what has been produced via it, is owned by BSM as a work tool. It is therefore forbidden to use the IT equipment and e-mails and internet for purposes and interests that are not strictly in line with those of BSM itself.

In compliance with the principles of relevance and non-excess, the checks on the IT equipment will be carried out by BSM in full respect of the fundamental rights and freedoms of the *Delegate* and in compliance with this Policy.

In the event of anomalies, BSM, as far as possible, will favour preliminary anonymous checks and therefore refer to aggregate data in the context of an entire department/area in which the anomaly occurred.

In case of successive, persistent anomalies, if necessary, BSM reserves the right to carry out checks on an individual basis, however, aimed exclusively at identifying any illicit conduct.

In no case will prolonged, constant or indiscriminate checks be carried out, without prejudice to checks to protect the interests of BSM itself.





**THE BRITISH SCHOOL OF MILAN**  
LEARNING TO EXCEL SINCE 1969

## GDPR & DATA PROTECTION POLICY

An audit is carried out by Deloitte to test the security of the system, with action points put into place following each audit.

### **Responsibilities and penalties**

The *Delegate*, in order not to expose themselves and BSM to the risk of sanctions, is required to adopt behaviours that are in compliance with current legislation and this Policy.

The *Delegates* are responsible for the correct use of internet and e-mail. Therefore they are responsible for damages caused to BSM's assets and reputation.

All *Delegates* are therefore required to observe and enforce the provisions contained in this Policy whose non-compliance or violation is a breach of contract and may result in:

- For employees the adoption of disciplinary measures provided for by the National Labor Contract and the civil and criminal actions established by the law;
- For third parties the termination of the contract and the civil and criminal actions established by the laws.

- This Policy should be read in conjunction with the the *Acceptable use Policy*

**Italian version follows – Segue versione Italiana**



## GDPR & DATA PROTECTION POLICY

### **Policy aziendale in materia di utilizzo degli strumenti informatici ed istruzioni operative per il trattamento dei dati ai sensi del GDPR 2016/679**

Il presente documento ha l'obiettivo di regolamentare l'utilizzo degli strumenti informatici per gli Incaricati di tali servizi nell'ambito della struttura aziendale all'interno di *The British School of Milan S.r.l* (di seguito *BSM*)

Le presenti regole di sicurezza si pongono l'obiettivo di fornire agli Incaricati idonee misure di sicurezza e linee di comportamento adeguate per utilizzare in modo conforme e non rischioso strumenti di comunicazione elettronici aziendali, la navigazione in internet e il trattamento dei dati in possesso della *BSM*.

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, la presente Policy è adattata in conformità alle regole emesse dal Regolamento UE 2016/679 per la tutela dei dati personali.

Copia della presente Policy viene consegnata a ciascun dipendente in essere e/o all'atto dell'assunzione ed a ciascun collaboratore ad inizio dell'attività con *BSM*. Per le terze parti che trattano dati in possesso della *BSM* è inoltre prevista la firma della delega per il suddetto processamento (*Appointment for data processing delegate*).

#### **Premessa**

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare il libero accesso alla rete internet attraverso i Personal Computers, espone la *BSM* ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine della *BSM* stessa.

Il presente documento viene incontro alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e collaboratori esterni e contiene informazioni utili per comprendere cosa può fare ogni Incaricato per contribuire a garantire la sicurezza informatica di tutta la *BSM*.

#### **Campo di applicazione**

La presente Policy si applica:

- A tutti i dipendenti e a tutti i collaboratori di *BSM* (di seguito congiuntamente denominati Incaricati) che si trovano ad operare sui dati personali di cui *BSM* stessa è titolare, a prescindere dal rapporto contrattuale con la stessa intrattenuto;
- A tutte le attività o comportamenti comunque connessi all'utilizzo della rete internet e degli strumenti di comunicazione elettronici, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale.

#### **Riferimenti normativi e definizioni**

Gli Incaricati sono le persone fisiche autorizzate, da parte del Titolare (*BSM*), a compiere operazioni di trattamento dei dati.



## GDPR & DATA PROTECTION POLICY

In particolare le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità di BSM, attenendosi alle istruzioni ricevute.

Si evidenzia, ai fini della presente Policy, che:

- Con il termine “trattamento” ci si riferisce ad una qualunque operazione effettuata sui dati con o senza l'ausilio di mezzi automatizzati che abbia come oggetto la raccolta, la registrazione, la consultazione, l'elaborazione, la modifica, la diffusione, l'estrazione la distruzione dei dati anche se non registrati nella banca dati;
- Con il termine “dato personale” si fa riferimento a qualunque informazione relativa a persona fisica o giuridica, ente o associazione, siano esse informazioni nominative o una qualunque altra informazione che possa rendere identificabile l'interessato;
- Con il termine “dato sensibile” si fa riferimento ai dati idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale dell'interessato;
- Con il termine “dato giudiziario” si fa riferimento ai dati idonei a rilevare i provvedimenti in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti.

Come indicato all'articolo 12 del **Regolamento della British School of Milan** la Scuola, in qualità di titolare del trattamento, tratterà i *dati personali di Richiedenti ed Associati e dei soggetti per cui è formulata Richiesta di Iscrizione alla Scuola*, **identificativi** (tra cui, nome, cognome, indirizzo, codice fiscale) ed eventualmente **sensibili** (malattia o stato di salute o intolleranze o allergie eventualmente comunicate alla Scuola), nel pieno rispetto delle norme di cui al Regolamento EU (GDPR) 2016/679.

Con la sottoscrizione del Modulo RIS, i dati identificativi sono trattati anche senza il consenso espresso del Richiedente e dell'Associato, per le seguenti **Finalità Accademiche**: esecuzione del Contratto (e quindi accettare la Richiesta di Iscrizione); gestione dei rapporti precontrattuali e contrattuali; adempimenti fiscali, gestione degli incassi e dei pagamenti; ottemperanza agli obblighi previsti da leggi, regolamenti o dalla normativa comunitaria ovvero imposti dalle Autorità ai fini dell'esecuzione del Contratto.

I dati identificativi e non sensibili sono trattati, solo previo distinto ed esplicito consenso, per le seguenti **Finalità di Promozione e Valorizzazione della Scuola**:

12.3.1. invio da parte della Scuola agli Associati di newsletter via email contenente informazioni, anche promozionali, relative alla Scuola e ad eventi ed attività organizzati dalla stessa;

12.3.2. pubblicazione dell'immagine fotografica e/o video dei soggetti per cui è formulata Richiesta di Iscrizione alla Scuola, scattata o ripresa durante eventi interno o esterni alla Scuola organizzati dalla Scuola, e/o del nominativo (mai contemporaneamente) dei soggetti stessi, nella brochure e/o nel materiale promozionale della Scuola e/o all'interno del Sito web e degli account social della Scuola. Ciò al solo ed unico scopo di promuovere la Scuola e di valorizzarne la sua attività.

12.4 I dati potranno essere resi accessibili per le finalità di cui all'art. 12.2 e 12.3 a dipendenti e collaboratori della Scuola, tra cui gli Associati che ricoprono il ruolo di Rappresentanti di classe, nella loro qualità di incaricati del trattamento; all'organizzazione degli Associati denominata “Amici della



## GDPR & DATA PROTECTION POLICY

Scuola” ed alle organizzazioni che operano per conto della Scuola, nella loro qualità di responsabili del trattamento e/o amministratori di sistema.

12.5 L'autorizzazione al trattamento dei dati per le finalità di cui all'art. 12.2 è obbligatorio; l'autorizzazione al trattamento dei dati per le finalità di cui all'art. 12.3 è invece facoltativo. Il mancato consenso per le finalità del punto 12.2 comporta l'impossibilità per la Scuola di accettare la Richiesta di Iscrizione e dare esecuzione al Contratto; il mancato consenso per le finalità promozionali del punto 12.3 invece non esclude l'accettazione da parte della Scuola della Richiesta di Iscrizione e la possibilità di dare esecuzione al Contratto.

L'elenco dei trattamenti effettuati, degli strumenti utilizzati, dei criteri utilizzati per il salvataggio ed il ripristino dei dati sono schematizzati all'interno del *Documento Programmatico sulla sicurezza* e del *Registro dei trattamenti effettuati*.

### **Linee guida**

La BSM detiene i dati personali dei suoi allievi, inclusi: i dettagli del contratto di iscrizione, i risultati di valutazione / esame, le informazioni sulla frequenza, i comportamenti positivi e negativi e le caratteristiche quali il gruppo etnico, le esigenze educative speciali, le informazioni mediche e le fotografie.

I dati vengono utilizzati per sostenere l'attività educativa degli allievi, per fornire un adeguato supporto pastorale e per valutare l'andamento complessivo di BSM.

Qualsiasi uso di dati personali relativi agli allievi, ai loro genitori o ai tutori per la raccolta di fondi, la pubblicità o la promozione deve essere fatto con esplicito consenso dell'interessato.

Di seguito vengono descritte le norme a cui gli incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto di trattamento, l'incaricato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa:

- Tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- Le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- In caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
- Non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;



## GDPR & DATA PROTECTION POLICY

- Devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
- Deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

### **Accesso ai dati dalla postazione di lavoro**

L'utilizzo del computer e della rete aziendale deve avvenire rispettando le seguenti indicazioni:

- Il personal computer affidato all'Incaricato è uno strumento di lavoro, ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione e il loro utilizzo deve avvenire per soli scopi legati alla propria attività lavorativa (mansioni)
- Non è consentito all'utente di modificare le caratteristiche hardware e software impostate sul computer assegnato dalla scuola, salvo previa autorizzazione del CFO;
- Se in possesso di un computer portatile non lasciarlo incustodito;
- Non lasciare incustoditi gli smartphones ed i tablets;
- Le informazioni archiviate digitalmente devono essere esclusivamente quelle necessarie all'attività lavorativa e solo su espressa autorizzazione del diretto Responsabile;
- Non utilizzare in BSM risorse informatiche personali per la raccolta, gestione e trattamento di dati in possesso della BSM
- Non connettere chiavette USB al personal computer o ad altri strumenti informatici aziendali;
- Non scaricare documenti aziendali sul computer personale;
- Non aprire documenti aziendali dal computer personale;
- Non utilizzare dispositivi personali (smartphones, tablets, fotocamere, etc) per scattare foto o girare video degli studenti di BSM;
- È vietato installare sul computer aziendale autonomamente programmi; infatti, esiste il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti e di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dalla BSM.
- Non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate;
- Non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente sicuri dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle;
- È fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati;
- È vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del CFO;
- È vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne alla BSM;
- È vietato condividere in rete cartelle con dati sensibili sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione del CFO;





## GDPR & DATA PROTECTION POLICY

- L'Amministratore di Sistema può, su espressa autorizzazione del CFO, procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui computer degli incaricati sia sulle unità di rete.

### **Gestione della password**

L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password) attribuito dall'amministratore di sistema che provvede inoltre alla gestione delle scadenze e delle caratteristiche della password.

Per una corretta gestione della password, ciascun incaricato deve aver cura di:

- Mantenerla riservata e non divulgarla a terzi
- Non permettere ad altri incaricati di operare con il proprio identificativo
- L'incaricato è tenuto a scollegarsi dal computer ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicato il computer;

Lasciare un computer/palmare incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

### **Internet e strumenti di comunicazione elettronici**

Gli strumenti di comunicazione telematica (internet e posta elettronica) devono essere utilizzati

solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno alla BSM. La casella di posta elettronica, assegnata dalla BSM all'incaricato è uno strumento di lavoro, le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

L'abilitazione all'uso della posta elettronica e la navigazione in Internet viene espressamente autorizzata dal CFO.

In particolare, l'incaricato dovrà osservare le seguenti regole:

- Nel caso di mittenti sconosciuti o messaggi insoliti per non correre rischi di essere infettati da virus occorrerà cancellare i messaggi senza aprirli
- l'incaricato deve utilizzare solo caselle di posta elettronica forniti dalla scuola per comunicare con alunni, genitori o tutori. Gli account di posta elettronica personali non possono essere utilizzati.
- È vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o dati critici senza garantirne l'opportuna protezione
- Le comunicazioni elettroniche inviate con caselle di posta elettronica scolastiche devono essere scritte in modo professionale e accurato.
- Il personale e gli studenti devono comunicare al proprio responsabile se ricevono e-mail offensive, minacciose o inadatte o all'interno della scuola o da posta esterna.



## GDPR & DATA PROTECTION POLICY

- Occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare. I destinatari e le modalità con cui sono autorizzati all'accesso dei dati BSM sono elencati di seguito:
  - Personale docente e non docente sono autorizzati dal contratto lavorativo;
  - Genitori di studenti della scuola sono automaticamente autorizzati dalla firma dei documenti di iscrizione;
  - Altri soggetti dovranno essere espressamente autorizzati
- La casella di posta deve essere tenuta in ordine cancellando documenti inutili ed eliminando allegati ingombranti
- Non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa
- Le caselle di posta elettronica degli studenti con il suffisso bsm.school devono essere utilizzati solo per la posta interna. Qualsiasi tipo di corrispondenza esterna deve essere autorizzata da un membro del personale, inserito in copia carbone (ad es. Per CAS o esperienza lavorativa).

### **Protezione antivirus**

I computer dati dalla BSM in dotazione agli incaricati, pur protetti contro gli attacchi dei virus informatici mediante appositi e sofisticati programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti.

Per ridurre la probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

- Chiudere correttamente i programmi in uso
- Non aprire se si lavora in rete file sospetti e di dubbia provenienza
- Non scaricare o installare applicazioni/software che non siano state preventivamente autorizzate
- Non utilizzare supporti elettronici di provenienza incerta
- Porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal computer

Alla verifica di un malfunzionamento del computer che può far sospettare la presenza di virus, è bene che l'incaricato

- Sospenda ogni operazione sul computer
- Chiuda il sistema e le relative applicazioni
- Contatti immediatamente l'Amministratore di sistema

### **Violazione dati personali**

La violazione dei dati personali è una violazione della sicurezza che causa la distruzione, perdita, alterazione accidentale o illegale, divulgazione non autorizzata o accesso a dati personali o dati di categorie speciali trasmessi, archiviati o altrimenti elaborati.



## GDPR & DATA PROTECTION POLICY

Esempi di violazione dei dati includono quanto segue:

- Perdita o furto di dati o apparecchiature su cui sono archiviati i dati, ad esempio la perdita di un laptop o di un file cartaceo (ciò include la perdita accidentale)
- Controlli di accesso inappropriati che consentono un utilizzo non autorizzato
- Errore umano (ad esempio l'invio di un'e-mail o un SMS al destinatario sbagliato)
- Hacking, phishing e altri attacchi in cui le informazioni vengono ottenute ingannando chi le detiene

In caso di violazione sospetta o accertata dei dati personali, qualsiasi dipendente deve segnalarla a:

- il Chief Financial Officer, Gianni Iaia, [gianni.iaia@bsm.school](mailto:gianni.iaia@bsm.school)
- il Direttore ICT, Andrea Lanuara, [andrea.lanuara@bsm.school](mailto:andrea.lanuara@bsm.school)

Ricevuta la segnalazione, il CFO ed il Direttore ICT effettueranno le ulteriori indagini approfondite e ne discuteranno con il DPO.

Sarà cura del DPO accertare se si sia effettivamente verificata una violazione dei dati personali e valutare se sia necessaria una specifica comunicazione all'Autorità.

La BSM identificherà quindi come si è verificata la violazione e prenderà misure immediate per fermare o ridurre al minimo l'ulteriore perdita, distruzione o divulgazione non autorizzata dei dati personali. La BSM identificherà i modi per recuperare, correggere o eliminare i dati (ad esempio notificando alla polizia se la violazione riguarda hardware o dati rubati).

### **Archivi cartacei**

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o comunque, ai non autorizzati al trattamento.

In caso di trattamento di dati sensibili tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanza chiusa a chiave in caso di allontanamento anche temporaneo dalla postazione di lavoro.

### **Accesso ai dati dell'utente**

L'Amministratore di sistema può accedere ai dati trattati dall'incaricato tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa.

Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, l'Amministratore di sistema accederà ai dati su richiesta dell'incaricato stesso e/o previo



## GDPR & DATA PROTECTION POLICY

adeguato avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, l'Amministratore di sistema avrà anche la facoltà di collegarsi e visualizzare in remoto le singole postazioni. Lo stesso Amministratore di sistema può, nei casi su indicati procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale.

L'Amministratore di sistema, in caso di assenza improvvisa o prolungata dell'incaricato o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è, su espressa autorizzazione del CFO, abilitato ad accedere alla posta elettronica dell'incaricato per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'incaricato.

L'Amministratore di sistema, su espressa autorizzazione del CFO, può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative. L'eventuale controllo sui file di log da parte dell'Amministratore di sistema non è comunque continuativo ed è limitato ad alcune informazioni, ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza della BSM e comunque non oltre i 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovrascrittura) i dati personali degli incaricati relativi agli accessi internet e al traffico telematico.

L'Amministratore di sistema, su espressa autorizzazione del CFO, è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'incaricato alla BSM per cessazione del rapporto, sostituzione delle apparecchiature ecc. Sarà cura dell'incaricato la cancellazione preventiva di tutti gli eventuali dati personali ivi contenuti.

In ogni caso viene garantito la non effettuazione di alcun trattamento mediante sistemi hardware e software, specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

- Lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per lo svolgere il servizio e-mail;
- riproduzione di eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

### **Uso di fotografie di singoli studenti**

La scuola segue le regole generali sull'uso delle fotografie dei singoli bambini:

- È necessario ottenere il consenso dei genitori. Il consenso riguarderà l'uso delle immagini in:
  - tutte le pubblicazioni scolastiche
  - sul sito web della scuola
  - sui giornali, come consentito dalla scuola
  
  - nei video realizzati dalla scuola o in classe per progetti scolastici
  - sui social media



**THE BRITISH SCHOOL OF MILAN**  
LEARNING TO EXCEL SINCE 1969

## GDPR & DATA PROTECTION POLICY

- Le immagini saranno scelte con cura per garantire che non presentino rischi di uso improprio.
- Per i documenti pubblici, inclusi i giornali, i nomi completi non saranno pubblicati accanto alle immagini del bambino.

### **Diritto di accesso ai propri dati personali e all'oblio**

Come indicato nel regolamento BSM, Art 12.6 I Richiedenti e gli Associati potranno accedere ai dati propri e dei soggetti per cui è formulata Richiesta di Iscrizione in qualsiasi momento ed esercitare i diritti di cui all'art. 15 del GDPR 2016/679.

I Richiedenti e gli Associati potranno in qualsiasi momento esercitare i diritti di cui all'art. 15 del GDPR 2016/679: inviando una email a [secretary@bsm.school](mailto:secretary@bsm.school).

Nella tabella seguente sono indicati i tempi e le modalità di distruzione dei dati a disposizione della BSM.





## GDPR & DATA PROTECTION POLICY

DATI GESTITI BSM: STUDENTI - GENITORI - DIPENDENTI			
DATI/DOC. STUDENTE	Distruzione dei dati / Documenti	DATI / DOC. DIPENDENTE	Distruzione dei dati / Documenti
Nome e Cognome	archivio	Nome e Cognome	10 anni
Certificato di Nascita	termine rapporto	Certificato di Nascita	termine rapporto
Codice Fiscale	archivio	Codice Fiscale	10 anni
Indirizzo Residenza	10 anni	Indirizzo Residenza	10 anni
Classe	archivio	Informazioni Mediche	termine rapporto
Data Iscrizione	archivio	Vaccinazioni	termine rapporto
Pagelle	archivio	Certificato Penale	termine rapporto
Rapporti Disciplinari	archivio	Curriculum Vitae	10 anni
Carta Identità	10 anni	Dati Coniuge	termine rapporto
Modulo Iscrizione	10 anni	Dati Figli	termine rapporto
Informazioni Mediche	termine rapporto	Lettera Assunzione	10 anni
Vaccinazioni	termine rapporto	Lettera Dimissioni	10 anni
		Lettera Incremento Stipendio	10 anni
		Referenze	10 anni
		Conto Bancario	termine rapporto
		Contratto affitto Appartamento	termine rapporto
		Passaporto / Carta Identità	10 anni
		Tessera Sanitaria	10 anni
DATI / DOC. GENITORI			
Nome e Cognome	10 anni		
Indirizzo Residenza	10 anni		
Cellulare	termine rapporto		
Email	termine rapporto		
Modulo Iscrizione Associazione	10 anni		
Sentenza di affidamento	10 anni		
Codice Fiscale	10 anni		
Carta Identità	10 anni		

### Controlli da parte della BSM

Si sottolinea che la strumentazione informatica e quanto con essa creato è di proprietà della BSM in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli della BSM stessa.



## GDPR & DATA PROTECTION POLICY

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dalla BSM nel pieno rispetto dei diritti e delle libertà fondamentali degli incaricati ed in osservanza della presente Policy.

In caso di anomalie, la BSM, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative nelle quali si è verificata l'anomalia.

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, la BSM si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.

In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi della BSM stessa.

### **Responsabilità e sanzioni**

L'incaricato, al fine di non esporre sé stesso e la BSM a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla presente Policy.

Gli incaricati sono responsabili del corretto utilizzo dei servizi di internet e Posta Elettronica. Pertanto sono responsabili per i danni cagionati al patrimonio ed alla reputazione di BSM.

Tutti gli incaricati sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nella presente Policy il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

- Per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi per tempo vigenti;
  - Per i collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.
- 
- Questo Procedimento deve essere letto contestualmente al Procedimento *Acceptable Use Policy*